FISC Security Reference Response Guide

Facility						
List of Measures in the FISC Security Guidelines						Responses to the Guideline
Item No.	Major Item	Medium Item	Minor Item	Concept of applicable location		Google Response
F1	IV Facility Guidelines I. Computer center	(I) Buildings (1. Environment)	F1 Avoid setting up a computer center in a place subject to disasters or failures	To reduce the influence of a disaster on a computer center, it is recommended to avoid setting up a computer center in a place subject to disasters and failures.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F2	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F2 Identify the potential of being subject to disasters and failures due to changes of site environment and develop proper preventive measures	To minimize the impact of any disaster on the computer center, it is recommended to identify the possibility of occurrence of disasters and failures due to changing natural environments and community environments and to develop proper preventive measures.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F3	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F3 Secure proper routes on the premises	Secure proper routes on the premises as specified in the Building Standards Act to facilitate the safe and secure fire-fighting activities and evacuation in the event of fire.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F4	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F4 Provide adequate clearance against adjacent structures	It is recommended to provide adequate clearance against adjacent buildings to prevent possible spread of fire and facilitate firefighting.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F5	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F5 Install walls or fences and equipment to prevent burglary	To prevent unauthorized entry into a site and destruction of a building, it is recommended to install walls or fences (and equipment to prevent burglary when necessary) when access control is performed at the borders of the site.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F6	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F6 Do not install a signboard, etc. outside	To prevent damage resulting from acts by outsiders such as trespassing and vandalism, it is recommended not to install a billboard or signboard outside indicating the existence or location of a computer center.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.

F7	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F7 Protect the buildings with proper lightning protection facility	To prevent possible failure or accident caused by lightning, it is recommended to protect the buildings with proper lightning protection facility in cases where there are no higher buildings in the neighborhood; otherwise the buildings would be located in any area subject to frequent lightning strike.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0" Google adheres to all building and facility requirements in the region where its data centers are located.
F8	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F8 Make the building available only for computer system-related operations, or establish an independent zone for computer system-related operations in a building	To ensure security control, it is recommended to dedicate the entire building to computer system-related operations or to establish an independent zone for computer system-related operations in a building.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.
F9	IV Facility Guidelines I. Computer center	(I) Buildings (2. Surroundings)	F9 Take measures to protect communication and power lines within a site from breakage and spread of fire	To prevent interruption of service provided by a computer system, it is recommended to take measures to protect communication and power lines within the site from breakage and spread of fire, which might be caused during some work activity or by an intruder from the outside.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F10	IV Facility Guidelines I. Computer center	(I) Buildings (3. Structures)	F10 Ensure that the buildings are fire-resistant	To ensure protection against fire, computer center buildings should be fire-resistant as per the Building Standards Act.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F11	IV Facility Guidelines I. Computer center	(I) Buildings (3. Structures)	F11 Ensure the safety of building structure	To protect the computer systems against possible failure, ensure the safety of building structure as per the Building Standards Act.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F12	IV Facility Guidelines I. Computer center	(I) Buildings (3. Structures)	F12 Ensure that building exterior walls, roofs, and other structural members are water-resistant	To protect the computer systems against possible failure, provide the exterior walls, roofs, and other structural members with proper precautions for prevention of water leakage.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F13	IV Facility Guidelines I. Computer center	(I) Buildings (3. Structures)	F13 Ensure adequate strength of exterior walls	To protect the computer-related equipment and facilities against vandalism, it is recommended to ensure sufficient strength of the exterior walls and other parts exposed to public roads.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
F14	IV Facility Guidelines I. Computer center	(I) Buildings (4. Openings)	F14 Ensure that the windows are provided with fireproofing capabilities	To protect against the spread of fire, ensure that the windows possibly exposed to fire spreading are provided with proper precautions for fire prevention.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F15	IV Facility Guidelines I. Computer center	(I) Buildings (4. Openings)	F15 Ensure that proper crime-prevention systems are installed	To protect the computer center buildings against unauthorized access, those windows on the ground floor that are easily accessible from the outside should be provided with proper crime-prevention systems.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
F16	IV Facility Guidelines I. Computer center	(I) Buildings (4. Openings)	F16 Designate only one entrance as a usual entrance, and install access control equipment and security equipment	To prevent unauthorized persons from entering and suspicious items from being brought in or taken out, through full implementation of access control, it is recommended to allow only one entrance to be usually used and ot install access control equipment and security equipment.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
F17	IV Facility Guidelines I. Computer center	(I) Buildings (4. Openings)	F17 Install emergency exits	To secure safe evacuation in the event of disaster and facilitate the smooth carrying out of property in an emergency, emergency exits shall be installed.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F18	IV Facility Guidelines I. Computer center	(I) Buildings (4. Openings)	F18 Provide proper waterproof measures	To protect the computer equipment and other facilities against failure caused by flooding and water leakage, it is recommended to protect the doorways, windows, ports for carrying equipment in/out, and other openings with proper waterproof measures.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F19	IV Facility Guidelines I. Computer center	(I) Buildings (4. Openings)	F19 Install entrance doors with sufficient strength and add locks	To prevent crimes and disasters, install doors with sufficient strength at an entrance and provide them with locks.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. Google adheres to all building and facility requirements in the region where its data centers are located.
F20	IV Facility Guidelines I. Computer center	(I) Buildings (5. Interior finish)	F20 Use building interior items made of non-combustible materials and having sufficient flame retardation efficiency	To ensure the protection of personnel and computer systems, use building interior items made of non-combustible materials in conformity with the Building Standards Act and having flame retardation efficiency in conformity with the Fire Service Act.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F21	IV Facility Guidelines I. Computer center	(I) Buildings (5. Interior finish)	F21 Make proper provisions for prevention of falling or broken interior items in the event of earthquake	To protect personnel and computer systems against possible damage, it is recommended to make proper provisions for prevention of falling or broken interior items in the event of earthquake.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F22	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (1. Location)	F22 Install the computer room and data storage room in proper locations that are less susceptible to disasters	Install the computer room and data storage room in proper locations that are less susceptible to earthquake, fire, flooding, or other disasters to prevent exposing the computer systems from possible impact.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F23	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (1. Location)	F23 Install the computer room and data storage room in proper locations inaccessible from the outside	To prevent unauthorized access, vandalism, and breach of secrecy, avoid the neighborhood of the entrance, and any locations allowing direct access by elevators or stairs for installation of the computer room and data storage room.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.
F24	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (1. Location)	F24 Do not install any signs indicating the names of rooms	To prevent unauthorized entry, vandalism, and breach of secrecy, do not put up any signs indicating the names of computers and data storage rooms.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.

F25	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (1. Location)	F25 Keep the necessary space	Keep the necessary space for maintenance, evacuation.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F26	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (1. Location)	F26 A computer room and a data storage room must be separate-dedicated rooms	A computer room and a data storage room must be separate-dedicated rooms in order to fully implement safety management.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F27	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (2. Openings)	F27 Designate only one entrance as a usually entrance, and provide it with a preparatory room	To fully implement access control, it is recommended to designate only one entrance as usually entrance. Also, to ensure safety and prevent external heat, humidity, and dust from entering, it is recommended to provide the entrance with a preparatory room.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F28	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (2. Openings)	F28 Install entrance doors of sufficient strength and add locks	To prevent crimes and disasters, install entrance doors of sufficient strength and provide them with locks.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F29	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (2. Openings)	F29 Apply fireproofing and waterproofing to windows, and take measures to prevent them from being broken and equipment in the room from being seen from the outside	To prevent crimes and disasters, apply fireproofing and waterproofing to windows, and take measures to prevent the windowpanes from being broken and equipment in the room from being seen from the outside.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F30	IV Facility Guidelines I. Computer center	(II) Computer Room and Data Storage Room (2. Openings)	F30 Install emergency exits, evacuation apparatus, and guide lights	To smoothly perform evacuation at the time of a disaster, install emergency exits and evacuation apparatus in appropriate places in a computer room. Also, install guide lights and guide signs to emergency exits.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F31	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (3. Structure and interior finish)	F31 Define the computer room and data storage room as independent fire retarding divisions	To protect the computer room and data storage room against possible fire spreading from the other divisions in the building, define the computer room and data storage room as independent fire retarding divisions as per the Building Standards Act.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environment health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F32	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (3. Structure and interior finish)	F32 Provide proper water leakage-prevention measures	To prevent possible damage to the building and facilities and possible failure of computer equipment, make proper provisions against water leakage from ceilings, walls, and floors.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F33	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (3. Structure and interior finish)	F33 Provide proper protection against static electricity	To protect the computer systems against adverse effects of static electricity, the materials for the surface of floor in the computer room should be properly prevented from occurrence of static electricity and the effects of electrostatic charge.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Google maintains an ESD program that includes training to applicable standards as well as prevention of ESD throughout the data center. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F34	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (3. Structure and interior finish)	F34 Use non-combustible and flame-proof materials for interior items	To protect personnel and computer systems against possible damage caused by fire, use proper noncombustible materials in conformity with the Building Standards Act and flame-proof materials in conformity with the Fire Service Act for the interior items.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environment health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F35	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (3. Structure and interior finish)	F35 Make proper provisions for prevention of possible falling or damage of interior items in the event of earthquake	To protect personnel and computer systems against possible damage, make proper provisions to prevent falling or damage of the partitioning walls, ceiling, lighting fixtures, and other elements that are likely to fall or be destroyed in the event of earthquake.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters. Google adheres to all building and facility requirements in the region where its data centers are located.
F36	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (3. Structure and interior finish)	F36 A free-access floor must be constructed as earthquake resistant, so that it is not damaged in the case of earthquakes	Undertake earthquake-proofing measures for free-access floors so that they are not damaged in the case of earthquakes.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F37	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F37 Install automatic fire alarm systems	To facilitate early detection and notification and initial firefighting and evacuation in the event of fire, install proper automatic fire alarm systems.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F38	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F38 Install proper communications systems in preparation for any emergency	To make a notification of a fire or other state of emergency and provide appropriate instructions about initial firefighting and evacuation, install proper communications systems for emergency use.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F39	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F39 Install fire extinguishing systems	In preparation for possible fire, install proper fire extinguishing systems.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
F40	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F40 Render the cables flame retardant and resistant to fire spreading	To prevent the cables from burning and spreading fire, it is recommended to render the cables flame retardant. In addition, protect the sections on the fire walls and the floor through which cables are installed with proper precautions against fire spreading.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F41	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F41 Install proper smoke exhaustion equipment	In preparation for a fire, install required smoke exhaustion equipment.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F42	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F42 Install proper emergency lighting equipment and portable lighting fixtures	To ensure the safe evacuation of personnel in the event of fire or other abnormal circumstances, provide proper emergency lighting equipment and portable lighting fixtures in the computer room.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F43	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F43 Do not install any equipment that uses water	Keep the computer systems away from impact due to water leakage; do not install any equipment that uses water in the computer room and data storage room.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F44	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F44 Install seismic detectors	To determine if it is appropriate to continue the operation of computer systems and prevent possibly destruction of data, electric fire, and/or other damage, installation of proper seismic detectors in the computer room is recommended.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google applies data center controls based on risk, including risks related to the region the data center is located. Where applicable, appropriate measures are taken to ensure that monitoring and management of natural and environmental disasters is taken, and that teams are trained to respond to local events. Google adheres to all building and facility requirements in the region where its data centers are located.

F45	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F45 Install access control and security facilities at entrances	To prevent unauthorized entry, install access control facilities to identify and record the entering/leaving of persons at the entrances of computer room and data storage room. Furthermore, security facilities are recommended to be installed.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.
F46	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F46 Install automatic temperature and humidity recorders or alarm systems for any exceptional temperature/humidity	For preventive maintenance of computer systems and identification of possible causes in the event of failure, install automatic temperature and humidity recorders or alarm systems for any exceptional temperature/humidity.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F47	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (4. Facilities)	F47 Make proper provisions against possible damage by rats	To protect cables against possible damage by rats, proper precautions are recommended.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google applies data center controls based on risk, including risks related to the region the data center is located. Where applicable, appropriate measures are taken to ensure that monitoring and management of natural and environmental disasters is taken, and that teams are trained to respond to local events. Google adheres to all building and facility requirements in the region where its data centers are located.
F48	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (5. Computer equipment, fixtures, and furnishings)	F48 Ensure that fixtures and furnishings are incombustible	To prevent ignition and spread of fire, furniture and fixtures should be made from steel or other incombustible materials.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F49	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (5. Computer equipment, fixtures, and furnishings)	F49 Provide proper protection against static electricity	To protect the computer systems against adverse effects of static electricity, computer equipment, fixtures and furnishings shall be provided with proper precautions against static electricity.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Google maintains an ESD program that includes training to applicable standards as well as prevention of ESD throughout the data center. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F50	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (5. Computer equipment, fixtures, and furnishings)	F50 Take proper precautions against possible earthquake	To protect personnel and computer equipment in the event of earthquake, provide computer equipment, fixtures and furnishings with proper earthquake-proof measures.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F51	IV Facility Guidelines I. Computer center	(III) Computer Room and Data Storage Room (5. Computer equipment, fixtures, and furnishings)	F51 Carriages, carts, and other equipment should be provided with proper locking devices	To protect personnel and computer equipment against possible damage in the event of earthquakes, carriages, carts, and other equipment for magnetic tape and magnetic disks shall be provided with proper braking or locking devices.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F52	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F52 Install the power supply room and air-conditioner room in a place less susceptible to disaster	To protect the computer systems against possible impact, the power supply room and air-conditioner room should be located in a proper place less susceptible to damage by disaster like earthquake, fire, or flooding.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.

F53	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F53 Provide adequate space for inspection and maintenance	For inspection and maintenance of equipment and systems, and also for secure evacuation in the event of disaster, provide space of required extent and height.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F54	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F54 Use independent, dedicated rooms for power supply room and air-conditioner room	To facilitate the maintenance and prevent possible spread of any failure, it is recommended to provide power supply room and air-conditioner room as dedicated rooms that are independent from other rooms.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F55	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F55 Do not install any windows, but install locked doors	To ensure the protection against intrusion from outside, fire prevention, and waterproofing, install locked doors, but no windows.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F56	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F56 Adopt fire-resistant structures	To prevent spread of fire in the event of fire, adopt fire-resistant structures.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F57	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F57 Install automatic fire alarm systems	For early detection of any fire, install automatic fire alarm systems.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F58	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F58 Install gas-based fire extinguishing systems	In preparation for any fire, it is recommended to install gas-based fire extinguishing systems of whole-are-release type.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F59	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F59 Take precautions against fire spreading from cables and ducts	To eliminate failure due to water leakage, take proper precautions against water leakage due to leakage of cooling water, leakage due to condensation, and other causes.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F60	IV Facility Guidelines I. Computer center	(III) Power Supply Rooms and Air-Conditioner Rooms	F60 Take proper precautions against fire spreading from cables and ducts	To prevent possible spread of fire, take proper precautions against fire spreading from cables and ducts.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F61	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F61 Allow an adequate margin for capacity of the power supply facilities	To ensure the steady supply of electric power to the computer systems, allow an adequate margin for capacity of the power supply facilities.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.

F62	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F62 Use multiple lead-in lines to draw in the power source	In preparation for possible failure in a power-receiving facility, using multiple lead-in lines to draw in the power source is recommended.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F63	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F63 Install a proper power supply facilities to supply electric power of high quality	To ensure that the computer systems can operate stably, install a proper power supply facilities that supplies electric power of high quality.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F64	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F64 Install a private power generation facility and a battery facility	A private power generation facility and battery facility should be installed to enable continued operation of the computer system even during power failure.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.

F65	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F65 Provide the power supply facilities with lightning protection facilities	To protect the power supply facilities against damage due to lightning strike, install lightning protection facility to the power supply facilities.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google applies data center controls based on risk, including risks related to the region the data center is located. Where applicable, appropriate measures are taken to ensure that monitoring and management of natural and environmental disasters is taken, and that teams are trained to respond to local events. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F66	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F66 Provide the power supply facilities with proper provisions against earthquake	To protect the power supply facilities against dislocation or damage in the event of earthquake, the power supply facilities should be provided with proper provisions against earthquake.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F67	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F67 Use dedicated equipment and lines to draw in the power source from a distribution board to computer devices	To minimize any hazardous influence on a computer system, draw in the power source from a dedicated distribution board to the computer devices through a dedicated circuit.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.

F68	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F68 Avoid combined use with any device involving significantly varying loads	To ensure the stable supply of electric power to the computer systems, use different power supply facilities between the computer system and any device involving significantly varying loads.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F69	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F69 Provide the computer systems with dedicated grounding	To ensure protection against possible disturbances from the power supply facilities, electrical machinery and apparatus, and other fixtures, ground the computer system appropriately.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F70	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F70 Make proper provisions against damage to each device due to over-current or leakage of electricity	To protect individual pieces of equipment against failure, make proper provisions against over-current or leakage of electricity.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F71	IV Facility Guidelines I. Computer center	(IV) Power supply facilities	F71 Install proper emergency power generators for disaster control and crime prevention systems	To ensure that disaster control and crime prevention systems can function properly even in the event of power failure, emergency power generators should be installed.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.

F72	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F72 Ensure that air-conditioning facilities have an adequate margin of capacity	To properly control the temperature and humidity in the computer room, ensure that air-conditioning facilities have an adequate margin of capacity.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F73	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F73 The air-conditioning facilities should have proper provisions for stable air conditioning	To ensure the consistent operation of computer systems, the air-conditioning facilities should have proper provisions for stable air conditioning.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F74	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F74 Use the air-conditioning facilities dedicated for the computer room	To precisely control temperature and humidity in the computer room, use a dedicated air-conditioning facilities for the computer room without any shared use with any other rooms.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F75	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F75 Install a backup air-conditioning facilities	In preparedness for occurrence of failure, installing backup machines for major air-conditioning facilities device is recommended.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F76	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F76 Provide the automatic control units and the emergency alarms for the air-conditioning facilities	To ensure that the air-conditioning facilities work consistently, provide various automatic control units and emergency alarms to detect any unusual conditions in device.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.

F77	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F77 Take measures against intrusion and destruction of air-conditioning facilities	To eliminate the occurrence of problems in the operation of a computer system, take measures against intrusion and destruction of air-conditioning facilities.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F78	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F78 Provide the air-conditioning facilities with proper protection against earthquake	To protect the air-conditioning facilities against possible movement or damage in the event of earthquake, the air-conditioning facilities should be equipped with proper earthquake-resistant measures.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F79	IV Facility Guidelines I. Computer center	(V) Air-conditioning facilities	F79 Insulation materials and air supply and exhaust openings for air-conditioning facilities should be made from noncombustible materials	To protect the air-conditioning facilities against damage in the event of fire, insulation materials for ducts in the air-conditioning facilities and air supply and exhaust openings should be made from noncombustible materials.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.

F80	IV Facility Guidelines I. Computer center	(VI) Monitor and Control System	F80 Install the monitor and control system	For early detection of any failure, install the monitor and control system for the power supply facilities, air-conditioning facilities, disaster control system, crime prevention system, and other systems.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F81	IV Facility Guidelines I. Computer center	(VI) Monitor and Control System	F81 Install the central control and monitoring station	To facilitate the management and control and the effective utilization of the power supply facilities, air-conditioning facilities, disaster control, crime prevention and other systems, installation of the central control and monitoring station is recommended for the centralized control of these systems.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F82	IV Facility Guidelines I. Computer center	(VII) Line-Related System	F82 Protect the line-related systems with proper locks	To ensure protection against unauthorized access, vandalism, and other unlawful acts, provide proper locks to the racks for line-related systems installed outside of the computer room.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.

F83	IV Facility Guidelines I. Computer center	(VII) Line-Related System	F83 Do not install any label to the line-related systems referring to indicate the installed location	To keep unauthorized persons from accessing the line-related systems, do not install any label to the line-related systems which indicate the installed locations.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F83-1	IV Facility Guidelines I. Computer center	(VII) Line-Related System	F83-1 Install the lines in the dedicated cabling space	To protect the lines against failure and crime and also interference from power cables and other cables, it is recommended to install the lines in a dedicated cabling space.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F84	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (1. Surroundings)	F84 Take proper precautions against broken wire and fire spreading for the telecommunications lines and power cables in the premises	To prevent possible interruption of computer system services, it is recommended to implement proper precautions for the telecommunications lines and power cables in the premises against wire breakage and fire spreading.		Out of Scope
F85	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (2. Structure)	F85 Ensure that the buildings are fire resistant	To ensure protection against fire, buildings shall be fire-resistant as the Building Standards Act.		Out of Scope
F86	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (2. Structure)	F86 Ensure the safety of building structure	To ensure the safety of building structure, buildings should meet the requirements of the building Standards Act.		Out of Scope
F87	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (2. Structure)	F87 Ensure that building exterior walls, roofs, and other structural members are water-resistant	To prevent water leakage, provide the exterior walls, roofs, and other structural members with proper water-resistant capabilities.		Out of Scope

F88	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (2. Structure)	F88 Ensure adequate strength of exterior walls	To ensure protection against destruction and unauthorized entry, it is recommended to ensure that the exterior walls and other parts exposed to public roads or to the outdoors are sufficiently strong.		Out of Scope
F89	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (3. Openings)	F89 Ensure that windows are provided with fireproofing capabilities	To ensure the protection against possible fire spreading, provide proper fireproofing precautions to the window possibly exposed to a risk of fire spreading.		Out of Scope
F90	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (3. Openings)	F90 Take proper precautions for windows and doors against crime	To ensure protection against unauthorized entry, windows and doors that are easily accessible from the outside should be provided with proper crime-prevention measures.		Out of Scope
F91	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (3. Openings)	F91 Ensure that entrance doors are sufficiently robust and they are protected with proper locks	For protection against crime and disaster, entrances should be equipped with proper doors with sufficient strengths and protected with locks.		Out of Scope
F92	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (3. Openings)	F92 Service entrances should be equipped with proper access control devices to identify any persons	To prevent unauthorized entry, service entrances used during out of business hours should be equipped with intercoms or other proper access control devices to allow identification of visitors from inside a room.		Out of Scope
F93	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (3. Openings)	F93 Entrances should be equipped with proper water-proof protection	To ensure the protection against inrush of rainwater, it is recommended that proper provisions be made for entrances against possible infiltration.		Out of Scope
F94	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (4. Interior finish)	F94 Ensure that ceilings and walls are thermal resistant and sound absorbing	To ensure correct functioning of terminal devices and other fixtures, making the ceilings and walls thermal resistant and sound absorbing is recommended.		Out of Scope
F95	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (4. Interior finish)	F95 Make proper provisions for prevention of possible falling or damaged interior items in the event of earthquake	To protect the human body and terminal devices and other property against damage in the event of earthquake, make proper provisions to prevent the ceilings, walls, lighting fixtures, and other articles which are likely to fall or suffer damage due to earthquake from falling or damage.		Out of Scope
F96	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (4. Interior finish)	F96 Floor surfaces should be constructed with proper materials causing less dust particles and static electricity	To protect terminal devices and other fixtures against adverse effects, it is recommended to construct the floor surfaces with proper materials causing less dust particles or static electricity.		Out of Scope
F97	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (4. Interior finish)	F97 Make proper provisions for the lines to terminal devices against possible wire breakage	To eliminate wire breakage when stamped underfoot by personnel, install the lines and power cables to terminal devices in proper locations.		Out of Scope
F98	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (4. Interior finish)	F98 Protect lines and power cables connected to terminal devices with proper precautions against water leakage	To eliminate possible interruption of system operation due to water leakage induced by any accident, it is recommended that lines and power cables connected to terminal devices be protected with proper precautions against water leakage.		Out of Scope

F99	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (5. Facilities)	F99 Install the automatic fire alarm systems and fire extinguishers	To facilitate early detection, immediate communication, initial firefighting and evacuation in the event of fire, install automatic fire alarm systems using smoke detectors or other proper equipment and also fire extinguishers.		Out of Scope
F100	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (5. Facilities)	F100 Take proper precautions against earthquake for individual fixtures	To protect terminal devices and other fixtures against damage, it is recommended that proper precautions against earthquake be taken for furniture and fixtures.		Out of Scope
F101	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (5. Facilities)	F101 Install fire-resistant safes	To minimize the impact of system failure caused by fire or other disasters, install fire-resistant safes, fire-resistant cabinets, and other proper data storage lockers for maintenance of the required media, documents, and data for restoration of normal operation.		Out of Scope
F102	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (5. Facilities)	F102 Install proper lightning protection facility	To protect the computer system against failure and the personnel within the building against electric shock and fatal wounds, and to prevent a risk of a fire and other accidents, it is recommended to install proper lightning protection facility in cases where no higher buildings are in the neighborhood.		Out of Scope
F103	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (5. Facilities)	F103 Crime-prevention measures should be implemented	The use of security cameras, emergency alarm systems, and other crime-prevention measures should be implemented in order to prevent crime before it occurs and to respond to crimes when they do occur.		Out of Scope
F104	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (6. Line-relate system)	F104 Do not install any sign to the line-related systems referring to indicate the installed locations	To keep the installed locations of line-related systems secret from unauthorized persons, do not install any sign to line-related systems showing the installed locations.		Out of Scope
F105	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (6. Line-relate system)	F105 Line-related systems should be provided with proper locks	To ensure protection against unauthorized access, vandalism, and other unlawful acts, proper locks should be installed to line-related systems, if they are easily accessible to any unauthorized persons.		Out of Scope
F106	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (6. Line-relate system)	F106 Cabling from line-related systems to individual terminal devices should be dual-redundant	To facilitate quick response to any line failure, it is recommended that the cabling from line-related systems to individual terminal devices be based on the dual-redundant design.		Out of Scope
F107	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (7. Power supply facilities)	F107 Install power cables properly with care not to interfere with terminal devices and other fixtures	To protect the terminal devices and other fixtures against interference, install power cables directly from the distribution board, or install the power cable properly with care so as not to disturb other equipment.		Out of Scope
F108	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (7. Power supply facilities)	F108 Install proper emergency power generators for disaster control and crime prevention systems	To ensure that disaster control systems, crime prevention systems, and emergency electric lighting systems can function properly even in the event of power failure, emergency power generators should be installed.		Out of Scope

F109	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (7. Power supply facilities)	F109 Private power generation facility and related facilities should be installed	It is recommended that private power generation facility and related facilities be installed in order to prepare for power failure.		Out of Scope
F110	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (8. Air conditioning facilities)	F110 Install air-conditioning facilities	To prevent malfunction of terminal devices and other fixtures, install the appropriate air-conditioning facilities for the number of pieces of terminal devices installed.		Out of Scope
F111	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F111 Install communication equipment	To quickly handle equipment failure in an ATM room, install communication equipment such as a telephone or an interphone in order to communicate with a working room when failure occurs.		Out of Scope
F112	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F112 Install emergency call systems	To quickly respond to any emergency situation in the ATM room, install emergency call systems for communications to the business office and other related divisions in an emergency.		Out of Scope
F113	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F113 Take proper precautions against possible crime	To ensure the security of ATM rooms, proper precautions against possible crime should be taken for the installed conditions and the environmental settings in the neighborhood by combining the security equipment for ATM room and the crime-prevention measures for the automatic equipment.		Out of Scope
F114	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F114 Install the lighting fixtures and emergency lighting systems	To prevent possible crimes in ATM rooms, install proper lighting fixtures offering sufficient light intensities to allow monitoring of the inside state of rooms from outside.		Out of Scope
F115	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F115 Install doors with see-through portions	To prevent various crimes, install doors with see-through portions so that the inside of the room can be seen from the outside.		Out of Scope
F116	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F116 Maintain the space necessary for the loading of cash into ATM, as well as for the maintenance of the equipment	For loading of cash into ATM and its maintenance, it is recommended that the necessary space be maintained at the rear side of the automated equipment.		Out of Scope
F117	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (9. ATM room)	F117 Install automatic operation facilities	To properly perform unattended automatic operation facilities, it is recommended to install the necessary automatic operation facilities.		Out of Scope
F118	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (10. Terminal devices)	F118 Protect terminal devices with proper earthquake-resistant measures	To protect terminal devices against possible dislocation and/or overturning and ensure the safety of personnel, it is recommended to take proper precautions against dislocation and overturning.		Out of Scope
F119	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (10. Terminal devices)	F119 Properly ground the device	For protection of device, establish a ground for the equipment requiring grounding from the distribution board.		Out of Scope
F120	IV Facility Guidelines II. Head offices / branch offices, etc.	(I) Buildings (10. Terminal devices)	F120 Protect the terminal devices against water leakage and dust particles	To protect the terminal devices against moisture and dust particles, provide waterproofing covers and/or other proper measures.		Out of Scope

F121	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (1. Location)	F121 Install server in zones that are safer against disasters	To prevent computer systems from suffering disasters, it is recommended to install servers in zones that are safer against earthquake, fire, floods, etc.		Out of Scope
F122	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (1. Location)	F122 Install servers in zones that are hard to access from outside	To protect servers against invasion, breakage, and unauthorized disclosure, it is recommended to avoid installing servers near the entrance of buildings or at places that are directly accessible through elevators or stairs.		Out of Scope
F123	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (1. Location)	F123 Do not install any sign showing the name of room where servers are installed	To prevent unauthorized access, vandalism, leakage of official secrets, and other events, it is recommended not to install any sign which identify the location of the server installed.		Out of Scope
F124	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (1. Location)	F124 Provide isolated rooms for installation of servers	For proper security control, it is recommended to provide isolated rooms for installation of servers.		Out of Scope
F125	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed locations (2. Structure & interior finish)	F125 Install the servers in the fire preventive blocks	To protect the servers against spread of fire from any other location in the building, it is recommended to install the servers in proper fire preventive blocks in conformity with the Building Standards Act.		Out of Scope
F126	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed locations (2. Structure & interior finish)	F126 Take proper precautions against water leakage	To protect the servers against damage due to water leakage, it is recommended to take proper precautions against water leakage from ceilings, walls and floors.		Out of Scope
F127	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed locations (2. Structure & interior finish)	F127 Protect the free access floors with proper earthquake retrofitting	It is recommended to protect the free access floors with proper earthquake retrofitting, in order to eliminate possible destruction.		Out of Scope
F128	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F128 Make the firefighting systems available	To protect the servers and other related equipment against fire damage, it is recommended to install the required firefighting systems.		Out of Scope
F129	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F129 install seismic detectors	To determine if it is appropriate to continue the operation of servers, it is recommended that proper seismic detectors be installed in the server-installed locations.		Out of Scope
F130	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F130 Install proper access control devices and crime-prevention equipment at the entrance of rooms where servers are installed	To prevent unauthorized access, it is recommended to install proper access control and crime-prevention devices at the entrance of rooms where servers are installed.		Out of Scope
F131	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F131 Install automatic temperature and humidity recorders or alarm systems for any exceptional temperature/humidity	For preventive maintenance of computer systems and identification of possible causes in the event of failure, it is recommended to install automatic temperature and humidity recorders or alarm systems for any exceptional temperature/humidity.		Out of Scope
F132	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F132 Install air-conditioning facilities	To ensure proper temperature and humidity conditions, it is recommended that dedicated air-conditioning facilities be installed.		Out of Scope
F133	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F133 Take measures to prevent damage by rats	It is recommended that appropriate measures be taken to prevent cables from being damaged by rats.		Out of Scope

F134	IV Facility Guidelines II. Head offices / branch offices, etc.	(II) Server-installed Locations (3. Facilities)	F134 Take measures for the preventing accidental pull-out of plugs connected with power point	To prevent plugs connected with power point from being easily pulled out of place, appropriate measures should be taken.		Out of Scope
F135	IV Facility Guidelines II. Head offices / branch offices, etc.	(III) In-Store Branch Offices	F135 Measures should be taken to prevent intrusion from other areas of the store	The area of the in-store branch should be an independent crime-prevention area separate from other parts of the store in order to prevent actions such as destructive intrusion.		Out of Scope
F136	IV Facility Guidelines II. Head offices / branch offices, etc.	(III) In-Store Branch Offices	F136 Appropriate reinforcement measures should be taken in stores that are used, according to their condition	When existing facilities in stores do not meet the same standards set for financial institutions, facilities should be reinforced and operational measures taken in order to prevent actions such as destructive intrusion.		Out of Scope
F137	IV Facility Guidelines III. Affiliated channels in distribution outlets and retail stores	(I) Convenience store ATMs	F137 Take proper precautions against possible rimes	To ensure the security of ATMs in convenience stores, proper precautions against possible crimes should be taken for the installed conditions and the environmental settings in the neighborhood by combining the security equipment and the crime-prevention measure for the ATMs.		Out of Scope
Operational						
Item No.	**Major Item**	**Medium Item**	**Minor Item**	**Concept of applicable location**		**Google Response**
O1	V. Operational Guidelines	Establishment of management systems (Security management and definition of responsibility)	O1 Documentation should be prepared with concrete definitions of security management methods.	Documentation that concretely specifies security management methods and defines responsibilities should be prepared in order to execute appropriate security management.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O2	V. Operational Guidelines	Establishment of management systems (Security management and definition of responsibility)	O2 Documentation that defines security management methods in concrete terms should be evaluated and revised.	In order to optimize security management methods, the documentation that has been created should be evaluated periodically in terms of its appropriateness to actual operations, and should be revised as necessary.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O3	V. Operational Guidelines	Establishment of management systems (Security management and definition of responsibility)	O3 Establish a security management system.	To properly perform security management, designate the persons, offices, etc. in charge of security management and define the scope of their tasks, authority, and responsibilities.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.

O4	V. Operational Guidelines	Establishment of management systems (Security management and definition of responsibility)	O4 Establish a system management system	To safely and smoothly operate a system and prevent illegal conduct, formulate system management procedures in order to establish a management system.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O5	V. Operational Guidelines	Establishment of management systems (Security management and definition of responsibility)	O5 Establish a data management system	To safely and smoothly manage data and prevent illegal conduct, formulate data management procedures in order to establish a management system.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O6	V. Operational Guidelines	Establishment of management systems (Security management and definition of responsibility)	O6 Establish a network management system	To properly and effectively operate computer networks and prevent unauthorized access, formulate network management procedures in order to establish a management system.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O7	V. Operational Guidelines	Establishment of management systems (Establishment of organization)	O7 Establish and maintain an organization for disaster prevention.	To prevent possible disaster and minimize the damage caused by any disaster, establish an organization for disaster prevention and define the assignment of responsibilities.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O8	V. Operational Guidelines	Establishment of management systems (Establishment of organization)	O8 Establish a proper crime prevention organization.	To ensure prevention of crime, establish a proper crime prevention organization and define the responsibilities and authority.		Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All employees agree to Google's Code of Conduct (https://abc.xyz/investor/other/google-code-of-conduct.html) and recieve training on Ethics and Compliance topics. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.

O9	V. Operational Guidelines	Establishment of management systems (Establishment of organization)	O9 Establish operational organizations.	To smoothly and properly manage the tasks related to a computer system and to prevent illegal conduct, define the scope of each task, responsibilities, and authority so as to establish a mutual check system.		Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All employees agree to Google's Code of Conduct (https://abc.xyz/investor/other/google-code-of-conduct.html) and recieve training on Ethics and Compliance topics. For customers using our Google Cloud Platform, they retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
O10	V. Operational Guidelines	Establishment of management systems (Formulation of regulations)	O10 Establish various regulations.	To smoothly and properly operate and manage a computer system, establish regulations that define the responsibilities and authority of each organization in charge of disaster-prevention, crime-prevention, and operation.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5), Organization of Information Security (ISO27001:2013, Annex A.6) and Operational Procedures and Responsibilities (ISO 27001:2013, Annex A 12.1) Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
O10-1	V. Operational Guidelines	Establishment of management systems (Confirmation of security observance.)	O10-1 Confirm the status of security observance.	To confirm the status of observance of items specified in security-related documentation, and to seek to raise the awareness of all officers and employees (including outsourcee's staff) regarding security policy and to improve their level of security.		Google is certified to the ISO27001 Standard, which regulates ""Information security awareness, education and training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
O11	V. Operational Guidelines	Physical access control (Physical access control (building and rooms))	O11 Establish proper authorization and key control systems.	To identify who enters the computer center, computer rooms, data storage rooms, and other sensitive rooms, implement proper access authorization and room key control.		"Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0"

O12	V. Operational Guidelines	Physical access control (Physical access control (building and rooms))	O12 Execute physical access control.	To prevent unauthorized entry, bringing-in of dangerous objects, and unauthorized carry-out, execute physical access control of a computer center building by verifying the visitors' authorization.		"Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0"
O13	V. Operational Guidelines	Physical access control (Physical access control (building and rooms))	O13 Execute room access control.	To prevent unauthorized entry, bringing-in of dangerous objects, and unauthorized carry-out, execute access control of important rooms such as computer rooms and data storage rooms by verifying the visitors' authorization.		"Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0"
O14	V. Operational Guidelines	Operational management (Documentation)	O14 Document and maintain manuals for operation in normal times.	To accurately and safely operate and manage the computer systems, prevent mishandling of terminal devices installed in the head offices and branch offices, and facilitate smooth office functions, various procedures (including those for system operation) in normal times should be documented and maintained in the form of manuals.		"Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (Annex A. 12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.

O15	V. Operational Guidelines	Operational management (Documentation)	O15 Prepare manuals used in case of a failure or disaster.	To minimize the influence of a failure or disaster of a computer system and to quickly recover as well as to continue operations in offices, prepare manuals that describe alternative measures, recovery procedures, and countermeasures in case of a failure or disaster.		"Google is certified to the ISO27001 Standard, which regulates "Protection of Records" (Annex A.12.1.1) and "Information Security Aspects of Business Continuity Management" (Annex A.17). Google maintains operational documentation to facilitate the recovery of systems. Documentation is located on systems that are replicated and subject to backup. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
O16	V. Operational Guidelines	Operational management (Access authority management)	O16 Definition of access authority to resources and systems.	For the protection against access by unauthorized persons, authorized persons who is allowed to access to computer systems and important files for system operation and business should be specified.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
O17	V. Operational Guidelines	Operational management (Access authority management)	O17 Take proper precautions not to make passwords known to anyone other than respective users.	To prevent possible leakage of passwords, proper precautions should be taken to not make them known to anyone.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
O18	V. Operational Guidelines	Operational management (Access authority management)	O18 Define the procedures for authorizing access to various resources and systems and reviewing the access authorization.	For proper control of access to various resources and systems, define the procedures for granting the access authorization. In addition, to properly keep the access authorization up to date, proper procedures should be established for renewing the access authorization.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

O19	V. Operational Guidelines	Operational management (Management of operations)	O19 Verify operator qualifications	Operator qualifications should be verified in order to prevent unauthorized use of computer systems.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
O20	V. Operational Guidelines	Operational management (Management of operations)	O20 Define the procedures for assignment and approval of operations.	To protect computer systems against unauthorized use, define the procedures for request and approval of operations.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
O21	V. Operational Guidelines	Operational management (Management of operations)	O21 Establish and maintain an organization for system operations.	To prevent mishandling and unauthorized use of computer systems, establish and maintain a system to implement the operations.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

O22	V. Operational Guidelines	Operational management (Management of operations)	O22 Make a record for checking of operations.	To verify the correctness of operations, make a record for checking of operations.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
O23	V. Operational Guidelines	Operational management (Management of operations)	O23 Manage operations in a client server-type system.	To prevent unauthorized use of a client/server system, it is necessary to clarify the procedures for request and approval, and appropriately manage such operations as execution, recording, verification of results. etc.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
O24	V. Operational Guidelines	Operational management (Input management)	O24 Manage data input.	To accurately process data and prevent unauthorized conduct, formulate input procedures.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.
O25	V. Operational Guidelines	Operational management (Data file management)	O25 Establish transfer and management methods.	To prevent unauthorized use, tampering, or loss of data files, transfer and store data files by following set procedures.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.
O26	V. Operational Guidelines	Operational management (Data file management)	O26 Define the procedures for revision control of data files.	To ensure the protection against unauthorized use and tampering, data files, if found inconsistent, should be properly revised and controlled based on the predefined procedures.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.

O27	V. Operational Guidelines	Operational management (Data file management)	O27 Maintain backup copies.	To cope with damage of important data files or in the event of a disaster, maintain backup copies, and specify their management method.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
O28	V. Operational Guidelines	Operational management (Program file management)	O28 Establish and maintain procedures for control of program files.	To protect every program against tampering, destruction, and other malicious acts, program files should be controlled in accordance with predetermined procedures.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support program file management activities.
O29	V. Operational Guidelines	Operational management (Program file management)	O29 Maintain backup copies.	To cope with destruction and failure of programs, maintain backup copies, and specify their management method.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support program file management activities.

O30	V. Operational Guidelines	Operational management (Measures against computer viruses)	O30 Take measure against computer viruses.	To cope with the invasion and infection of computer viruses, definite procedures for protection, detection, and recovery should be made.		Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate protective measures against viruses.
O31	V. Operational Guidelines	Operational management (Network setting information management)	O31 Implement configuration management.	Management of configuration of network device should be implemented to protect them against tampering.		"Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O32	V. Operational Guidelines	Operational management (Network setting information management)	O32 Maintain backup copies of configuration.	To cope with unauthorized changes of configuration, failures or disasters maintain backup copies of configuration and specify their management method.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

O33	V. Operational Guidelines	Operational management (Document management)	O33 Storage management should be defined.	Documents should be managed using established methods in order to prevent unauthorized use, tampering loss, etc.		Google is certified to the ISO27001 Standard, which regulates "Protection of Records" (ISO 27001:2013, Annex A. 12.1.1). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support storage management.
O34	V. Operational Guidelines	Operational management (Document management)	O34 Maintain backup copies.	In preparation for the restoration operation from a disaster, make backup copies of documents necessary for the operation and specify their management method.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support forms management.
O35	V. Operational Guidelines	Operational management (Forms management)	O35 Establish a method for managing unused important forms.	To prevent unauthorized use of unused important forms, perform their inventory control and destruction by using established methods.		Responsibility for developing a process to support forms management rests with the customer.
O36	V. Operational Guidelines	Operational management (Forms management)	O36 Establish and maintain the procedures for handling of important printed forms.	To ensure protection against unauthorized use, follow the specified procedures for transfer and discarding of important printed forms.		Responsibility for developing a process to support forms management rests with the customer.
O37	V. Operational Guidelines	Operational management (Output management)	O37 Take measures for the prevention from unauthorized actions and the protection of secrecy in making and handling output information.	For the prevention from tampering, burglary, and leaks, measures should be taken for the prevention of unauthorized actions and the protection of secrecy in making and handling output information.		Responsibility for developing a process to support output information rests with the customer.
O38	V. Operational Guidelines	Operational management (Transaction management)	O38 Define operational authority for each transaction.	To prevent illicit transactions through the operation of terminal devices, define the scope of operational authority of terminal operators for each transaction.		Responsibility for transaction management rests with the customer.
O39	V. Operational Guidelines	Operational management (Transaction management)	O39 Properly control the operator cards.	To prevent unauthorized transactions through the operation of terminal devices, designate the administrators for proper control of operator cards.		Responsibility for transaction management rests with the customer.
O40	V. Operational Guidelines	Operational management (Transaction management)	O40 Keep a log of operations for transactions and inspect the log.	To prevent unauthorized transactions through operation of terminal device, establish and maintain a proper system to allow verification of transactions based on statement of account, log of operations of terminal device, and other records.		Responsibility for transaction management rests with the customer.

O41	V. Operational Guidelines	Operational management (Transaction management)	O41 Establish for reception system of reports from customers, and implement the management of troubled accounts.	In order to prevent unauthorized use resulting from troubles, a system should be established for reception of reports of theft, etc. of device and media that are capable of linking to accounts and transferring customer assets. Management of accounts reported as troubled should also be carried out using established methods.		Responsibility for transaction management rests with the customer.
O42	V. Operational Guidelines	Operational management (Transaction management)	O42 State the loss that a user may suffer, and his or her responsibility accompanying the theft or damage of equipment or a medium.	To call the user's attention to his or her responsibility, clearly state the loss that a user may suffer and his/her responsibility accompanying the theft or damage of a medium that stores electronic values, and equipment used for communications.		Responsibility for transaction management rests with the customer.
O43	V. Operational Guidelines	Operational management (Cryptographic keys management)	O43 Operational management methods should be defined for the use of cryptographic keys.	Procedures should be established for the generation, distribution, use, storage, etc. of cryptographic keys that are used, in order to prevent unauthorized actions. The documents for managing these procedures also should be strictly controlled by the officer in charge.		Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing cryptographic key management processes.
O44	V. Operational Guidelines	Operational management (Strict ID confirmation)	O44 Implement personal identification.	At the time of opening an account of Internet banking or other transactions that take place without face-to-face interaction, confirm identity based on a proper method.		Responsibility for validation of identity rests with the customer.
O44-1	V. Operational Guidelines	Operational management (Transaction management)	O44-1 Ensure the financial transactions by duly authorized customers in the cash transactions through CD/ATM, and other automated machines.	Ensure that deposit withdrawals and other cash transactions through CD/ATM, and other automated machines are properly performed for duly authorized customers, by taking appropriate precautions against possible illicit withdrawals.		Responsibility for validation of cash transactions via CD/ATM rest with the customer.
O45	V. Operational Guidelines	Operational management (Management of CD/ATM, and unmanned branches)	O45 Establish operational management methods and take appropriate precautions against Possible illicit withdrawals.	To ensure the security of CD/ATM, and unmanned branches, and for their smooth operation, establish operational management methods.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O46	V. Operational Guidelines	Operational management (Management of CD/ATM, and unmanned branches)	O46 Establish and maintain proper monitoring systems.	To detect any unusual conditions in automated branches, establish and maintain proper monitoring systems.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O47	V. Operational Guidelines	Operational management (Management of CD/ATM, and unmanned branches)	O47 Definition of the security systems.	For the prevention from crimes at unmanned branches, definite security methods should be established and countermeasures at the occurrence of crimes should be prepared.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O48	V. Operational Guidelines	Operational management (Management of CD/ATM, and unmanned branches)	O48 Establish and maintain proper preparedness for any failure or disaster.	To ensure the smooth operation of unmanned branches, establish and maintain proper preparedness for any failure or disaster.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O49	V. Operational Guidelines	Operational management (Management of CD/ATM, and unmanned branches)	O49 Document and maintain required manuals.	To ensure the smooth operation and secure safety of unmanned branches, document and maintain proper manuals referring to actions to be taken under various conditions.		Responsibility for CD/ATM and unmanned branches rests with the customer.

O50	V. Operational Guidelines	Operational management (Management of handheld terminals)	O50 Establish and maintain proper procedures for operation and management.	For protection of handheld terminals against possible unauthorized use, establish and maintain proper procedures for operation and management.		Responsibility for handheld terminals rests with the customer.
O51	V. Operational Guidelines	Operational management (Management of cards)	O51 Establish a method for managing cards.	To ensure security and to smoothly perform each operation concerning cards, follow set procedures for issuing, storing, granting, retrieving, and destroying cards.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O51-1	V. Operational Guidelines	Operational management (Management of cards)	O51-1 Raise customers' awareness about crimes.	To secure the safety of customers and transactions, raise customers' awareness about crimes.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O52	V. Operational Guidelines	Operational management (Management of cards)	O52 Define the procedures for monitoring transactions by using card in any designated accounts.	To ensure protection against unauthorized use, establish and maintain the procedures for monitoring transactions by using card in any designated account.		Responsibility for CD/ATM and unmanned branches rests with the customer.
O53	V. Operational Guidelines	Operational management (Protection of customer data)	O53 Take measures for the protection of customer data.	For the protection of customer data and proper use, management methods and procedures should be taken.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. Customers must also secure their own data, and retain full responsibility for its protection.
O53-1	V. Operational Guidelines	Operational management (Protection of customer data)	O53-1 Implement the security control measures for biometric information handled in the process of biometric authentication.	Establish and maintain the procedures for safe control of the biometric information when used in the personal identification of customers.		Customers are required to secure their user's biometrics data, when used.
O54	V. Operational Guidelines	Operational management (Resource management)	O54 Check individual resources for the capability and usage.	To avoid failure and degradation in throughput of computer systems, identify the capacity and usage of each resource and implement adequate measures.		"Google is certified to the ISO27001 Standard, which regulates "Capacity Management" (ISO 27001:2013, Annex A. 12.1.3). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including resource management.
O55	V. Operational Guidelines	Operational management (External connection management)	O55 Define the conditions of contract for external connection.	For secure and accurate external connection, define the connection methods, data format, data contents, and other elements before conclusion of any contracts for data transmission through line connections.		Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including management of external connections.

O56	V. Operational Guidelines	Operational management (External connection management)	O45 Establish operational management methods for external connections.	To prevent leakage of data and unauthorized access, establish operational management methods for external connections, such as how to identify the connect-to party and how to manage registration and alteration of connection conditions (passwords, etc.)		Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" (ISO 27001:2013, Annex A.14.1.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including management of external connections.
O57	V. Operational Guidelines	Operational management (Devices management)	O57 Definition of management method.	For the prevention of unauthorized use, breakage, etc. theft of computer system constituting devices, management by stipulated methods should be implemented.		Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
O58	V. Operational Guidelines	Operational management (Devices management)	O58 Take measures to protect network-related devices.	It is recommended that appropriate protective measures be taken with network device that handles important data as a component of the system, in order to prevent its unauthorized use, destruction, theft, etc.		Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
O59	V. Operational Guidelines	Operational management (Devices management)	O59 Define the procedures for maintaining the devices.	To prevent failure in the each device that constitute the computer systems, maintenance and inspection should be implemented and the inspection items and results should be identified.		Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2.4).
O60	V. Operational Guidelines	Operational management (Monitoring of operation)	O60 Establish proper monitoring systems.	For early detection of any unusual conditions, predetermine the targets for monitoring, monitoring items, and monitoring procedures.		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage and monitor their environment.

O61	V. Operational Guidelines	Operational management (Computer room and data storage room management)	O 61 Operations conducted after entry into the room should be managed.	The activities of people who enter important areas such as computer rooms and data storage rooms must be managed in order to prevent unauthorized intrusion, introduction of items that pose danger, unauthorized removal of property, etc.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.
O62	V. Operational Guidelines	Operational management (Measures for handling failures and disasters)	O62 Define the procedures for communicating with those who are responsible for control of failure and disaster.	To ensure the immediate and secure communications with those who are designated for control of failure and disaster in the event of failure and disaster, establish and maintain the procedures for proper communications.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O63	V. Operational Guidelines	Operational management (Measures for handling failures and disasters)	O63 Establish definite measures against failures and disasters.	Establish the definite measures against failures and disasters to recover the computer system which is not working properly due to failure and disaster. Such measures should correspond to contingency plans.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

O64	V. Operational Guidelines	Operational management (Measures for handling failures and disasters)	O64 Identify and analyze possible causes of any failure.	To facilitate quick recovery from failure, proper methods should be established for identifying possible causes of failures. In addition, the identified causes of failures should be recorded for trend analysis and other investigations to prevent recurrence.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O65	V. Operational Guidelines	Operational management (Formulate contingency plans)	O65 Formulation of a contingency plan.	Contingency plans (emergency response plans) should be formulated in advance to minimize the extent of damage and its impact on operations when unforeseen disaster, accident, failure, etc. has caused serious damage making it difficult to sustain system operations, and to facilitate speedy recovery.		Google is certified to the ISO27001 Standard, which regulates "Information Security Continuity" (ISO 27001:2013, Annex A.17.1). Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google also maintains a robust internal DR program, including development of appropriate contingency plans. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing appropriate contingency plans.
O66	V. Operational Guidelines	System development and modification (Hardware and software management)	O66 Hardware and software management should be performed.	Hardware and software configuration management and version management should be carried out in order to conduct system implementation, modifications, and disposal without errors.		Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (Annex A.8.1), "Disposal of Media" (Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (Annex A.11.2.7) and "Control of Operational Software (Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.

O67	V. Operational Guidelines	System development and modification (Hardware and software management)	O67 Establish definite development and modification procedures.	Establish definite development and modification procedures in order to assure the validity of the implementation.		Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O68	V. Operational Guidelines	System development and modification (Hardware and software management)	O68 Establish proper test environments.	To ensure the security of production systems, establish proper test environments that do not affect the production environments.		Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O69	V. Operational Guidelines	System development and modification (Hardware and software management)	O69 Define procedures for transition to production.	In order to assure the security of production systems, the characteristics of each system should be considered and transition procedures should be established when making the transition to production, and the consistency of procedures in related divisions should be confirmed.		Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O70	V. Operational Guidelines	System development and modification (System development and modification management)	O70 Establish the procedures for preparing system documents.	For successful preparation of system documents, define the items included in the documents and the procedures for preparing the documents.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5), Organization of Information Security (ISO27001:2013, Annex A.6) and Operational Procedures and Responsibilities (ISO 27001:2013, Annex A 12.1) Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including management of system documents.
O71	V. Operational Guidelines	System development and modification (System development and modification management)	O71 Define the procedures for proper storage management.	To facilitate the smooth utilization of documents and ensure the protection against tampering or unauthorized use of documents, implement proper storage management for system documents.		Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5), Organization of Information Security (ISO27001:2013, Annex A.6) and Operational Procedures and Responsibilities (ISO 27001:2013, Annex A 12.1) Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including storage management procedures.
O72	V. Operational Guidelines	System development and modification (Package installation)	O72 Establish a proper evaluation organization.	To facilitate the development or modification of systems for introduction of packages, establish a proper organization for evaluation of effectiveness, reliability, productivity, and other factors.		"Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
O73	V. Operational Guidelines	System development and modification (Package installation)	O73 Establish and maintain proper operation and management organization for packages.	To facilitate the development or modification of systems for introduction of packages, establish a proper organization.		"Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.

O74	V. Operational Guidelines	System development and modification (Disposal of systems)	O74 Establish a disposal plan and a disposal procedure for systems.	To perform smooth, correct and safe disposal of a system, it is necessary to establish a disposal plan and a disposal procedure which include measure to prevent unauthorized conducts and to protect secrecy, under the approval of a person responsible for operations and users.		Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A. 8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
O75	V. Operational Guidelines	System development and modification (Disposal of systems)	O75 Take measures to prevent the leakage of information.	In order to protect confidentiality and prevent unauthorized use of data, measures should be taken to prevent the leakage of information from devices at the time of disposal.		Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
O76	V. Operational Guidelines	Facility management (Maintenance and management)	O76 Establish a method for managing facilities.	To smoothly operate a computer system, specify persons responsible for the management of facilities and the management method, and manage the system by following a set procedure. Also, specify the actions on how to handle failures and disasters.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0

O77	V. Operational Guidelines	Facility management (Maintenance and management)	O 77 Establish and maintain proper procedures for maintenance of facilities.	To ensure the smooth operation of computer systems, implement maintenance and inspection and identify the inspection items and results.		Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001: 2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
O78	V. Operational Guidelines	Facility management (Resource management)	O78 Identify available capabilities and actual conditions of use.	For early detection of any unusual conditions, identify the capacity and performance limits of each facilities and the actual usage.		Google is certified to the ISO27001 Standard, which regulates "Capacity Management" (ISO 27001:2013, Annex A. 12.1.3). Google has a robust network that monitors and adjusts capacity on an as-needed basis worldwide.
O79	V. Operational Guidelines	Facility management (Monitoring)	O79 Establish and maintain a proper monitoring organization.	For early detection of any unusual conditions, define the points to be monitored, monitoring items, and monitoring methods.		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
O80	V. Operational Guidelines	Education and training (Education and training)	O80 Carry out security training.	For the enhancement of security awareness, security training of all officers and employees (including outsourcee's staff) should be implemented by making them understand security policy and specific security measures taking the personnel's responsible work into account.		Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

O81	V. Operational Guidelines	Education and training (Education and training)	O81 Carry out education to improve skills of personnel.	Education to improve knowledge and skills related to systems and the applications that are the subject of systems development should be carried out with consideration for the specific nature of the operations handled by the personnel in question.		Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O82	V. Operational Guidelines	Education and training (Education and training)	O82 Provide proper education and training for mastering system operation.	To ensure the smooth operation of computer systems under normal conditions and the mastery of operation of terminal devices for work in branch offices, provide proper education and training.		Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O83	V. Operational Guidelines	Education and training (Education and training)	O83 Provide proper education and training for possible failures and disasters.	In preparation for any failures and disasters, implement proper education and training about operation of computer systems.		Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O84	V. Operational Guidelines	Education and training (Education and training)	O84 Implement disaster prevention and crime prevention training.	Implement disaster prevention and crime prevention training against emergency.		Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

O85	V. Operational Guidelines	Staff management (Staff management)	O85 Appropriately perform personnel management.	To smoothly operate a system, appropriately perform personnel management such as arrangement and replacement of staff members.		Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including human resource management.
O86	V. Operational Guidelines	Staff management (Staff management)	O86 Implement proper health care management for employees.	Implement proper health care management for employees, including the improvement of working environments and regular medical examinations.		Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including human resource management.
O87	V. Operational Guidelines	External outsourcee management (External outsourcee management)	O87 Before outsourcing of computer systems development and operation, define the objectives and extent of outsourcing.	Before outsourcing the computer systems development and operation, the objectives and extent of outsourcing should be defined.		Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A. 15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. https://cloud.google.com/terms/subprocessors https://G Suite.google.com/terms/subprocessors.html
O87-1	V. Operational Guidelines	External outsourcee management (External outsourcee management)	O87-1 Establish an outsourcee selection rule and contracting procedures.	For selection of outsourcees, the procedures should be established and the outsourcees should be objectively evaluated. For selection of outsourcees, approval should be obtained from responsible personnel.		Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A. 15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. https://cloud.google.com/terms/subprocessors https://G Suite.google.com/terms/subprocessors.html

O88	V. Operational Guidelines	External outsourcee management (External outsourcee management)	O88 Conclude proper contracts for outsourcing, including the security control items.	To ensure security, conclude proper contracts for outsourcing, including the items relating to protection of corporate secrets and safe operation.		Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A. 15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. https://cloud.google.com/terms/subprocessors https://G Suite.google.com/terms/subprocessors.html
O89	V. Operational Guidelines	External outsourcee management (External outsourcee business management)	O89 Strict observance of rules by external outsourcee's staff should be assured, and the state of their observance should be managed and confirmed.	External outsourcee's staff should be made responsible for observance of security policy and other rules, and training and auditing should be conducted in order to carry out appropriate security management of external outsourcee's staff in a manner suited to the content and scope of outsourced operations.		Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O90	V. Operational Guidelines	External outsourcee management (External outsourcee business management)	O90 Establish an operational organization for externally outsources operations, and manage and confirm the work done.	An operational organization should be established in order to verify the content of work performed by external outsourcee, and management and confirmation should be performed on the basis of the work contract.		Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A. 15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
O90-1	V. Operational Guidelines	External outsourcee management (External outsourcee business management)	O92-1 Suitable risk management should be carried out where system network services are shared by Financial Institutions.	System network services shared by financial institutions are core infrastructure for financial institutions to settle financial transactions, and to develop CD/ATM networks. As faults in the system network may affect the entire settlement system and customer services, proper risk management is required.		Google does not maintain financial transaction software for customers. The responsibility of maintaining CD/ATM networks remains with the customer.
O91	V. Operational Guidelines	System auditing (System auditing)	O91 Establish system auditing structures.	To establish a system audit organization for the purpose of tracking and evaluating computer systems and systems management in terms of their effectiveness, efficiency, reliability, conformity, and safety.		Google is certified to the ISO27001 Standard, which regulates "Information Systems Audit Considerations" (ISO 27001:2013, Annex A.12.7), Information security oversight and management controls, including the establishment of internal audit oversight are reviewed and verified by a third party auditor for Google's SOC 2, Type II report
O92	V. Operational Guidelines	In-store branches	O92 Selection criteria should be defined for stores where branches are located.	Branch location area and store selection criteria should be defined in order to assure the security of in-store branches.		Responsibility for in-store branches rests with the customer and it out of scope for Google's platform.

O93	V. Operational Guidelines	ATM in convenience store	O93 Selection criteria for store locations should be defined.	Store location are and convenience store selection criteria should be defined in order to assure the security of an ATM in convenience store and their users.		Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O94	V. Operational Guidelines	ATM in convenience store	O94 Crime-prevention measures should be implemented during cash loading and other maintenance.	It is necessary to define a crime-prevention system and methods to assure security when maintaining an ATM in convenience store.		Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O95	V. Operational Guidelines	ATM in convenience store	O95 Procedures for response to failure and disaster should be defined.	Procedures should be defined for prompt response to failure and disaster at ATM in convenience store.		Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O96	V. Operational Guidelines	ATM in convenience store	O96 Security measures for network-related devices and data transmissions should be implemented.	Appropriate protective measures for network-related equipment and security measures for data transmissions should be implemented in order to assure the security and reliability of data transmissions and to prevent unauthorized use, destruction, falsification, etc.		Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O97	V. Operational Guidelines	ATM in convenience store	O97 A notification system should be established for contacting to the police that has jurisdiction and at security companies, etc.	A notification system should be established for contacting to the police that has jurisdiction and at security companies, etc. and training in it should be conducted in order to enable prompt notification of persons concerned when a crime occurs.		Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O98	V. Operational Guidelines	ATM in convenience store	O98 Take steps to make ATM customers cautious about crime.	It is recommended that such measures be implemented with regard to crimes directed against ATM customers in order to assure the security of users.		Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O99	V. Operational Guidelines	Debit card (Assure security of debit card services)	O99 Security measures should be taken for debit card services	Financial institutions should implement security measures jointly with information processing centers, affiliated stores, etc. in a manner suited to the format of services provided in order to assure the security of debit card services.		Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O100	V. Operational Guidelines	Debit card (Assure security of debit card services)	O100 Assure the security of account numbers, personal identification numbers, etc.	Financial institutions should implement security measures jointly with information processing centers, affiliated stores, etc. in a manner suited to the format of services provided in order to assure the security of account numbers, secret codes, etc.		Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O101	V. Operational Guidelines	Debit card (Customer protection)	O101 Measures should be taken to protect customers when they use debit cards.	Appropriate measures should be taken to protect customers to assure their security when they use debit cards.		Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O102	V. Operational Guidelines	Debit card (Make customers exercise caution)	O102 Steps should be taken to make customers exercise caution on certain points regarding the use of debit cards.	Customers should be explicitly informed about certain points regarding the use of debit cards, in order to make customers exercise caution.		Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O103	V. Operational Guidelines	Financial services using open networks (Internet and mobile services)	O103 Unauthorized use should be prevented.	Preventive measures to verify the identity of the connected part, access restrictions, detection measures, and other functions to prevent unauthorized use should be implemented in order to assure the security of financial services that utilize open networks.		Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.

O104	V. Operational Guidelines	Financial services using open networks (Internet and mobile services)	O104 Unauthorized use should be detected promptly.	Functions whereby users can confirm their usage status for themselves should be implemented in order to protect users against unauthorized use.		Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O105	V. Operational Guidelines	Financial services using open networks (Internet and mobile services)	O105 Conduct information disclosure regarding security measures.	It is recommended that disclosure of information regarding security measures be conducted in order to enable user to make appropriate selection of trading institutions and financial services.		Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O105-1	V. Operational Guidelines	Financial services using open networks (Internet and mobile services)	O105-1 Establish and maintain proper provisions for customer services.	In the financial services via the Internet, mobile telephone and other means, establish and maintain proper provisions for customer services such as attention attraction and points of contact for responding to customer inquiries.		Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O106	V. Operational Guidelines	Financial services using open networks (internet and mobile services)	O106 Define operations management methods.	Operations management methods should be defined in order to protect users, assure security, and provide smooth operations when conducting financial service transactions using the Internet, mobile services, etc.		Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O107	V. Operational Guidelines	Financial services using open networks (Email services)	O107 Define email operations policy.	Email operations policy should be defined in order to assure the reliability and security of email operation.		Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O108	V. Operational Guidelines	Use of cloud services	O108 When using cloud services, clarify the purpose, scope, etc. in advance, and clarify the procedures for selecting a cloud service provider.	When using cloud services, the purpose, scope, etc. should be clarified in advance, and the procedures for selecting a cloud service provider should be clarified and, in addition to that, providers should be evaluated objectively. The approval of the person responsible should be obtained when deciding on a cloud service provider.		Due diligence in selection of a cloud provider is an end-user responsibility. Google provides public-facing information regarding its offerings to allow potential customers to evaluate specific products.
O109	V. Operational Guidelines	Use of cloud services	O109 Establish a contract with a cloud service provider that includes items related to security measures.	Establish a contract that includes items related to the protection of confidential information, stable system operation, etc. in order to ensure security.		Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://G Suite.google.com/terms/2013/1/premier_terms.html SLA: https://G Suite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
O110	V. Operational Guidelines	Use of cloud services	O110 Take measures to prevent leakage of data when using cloud services.	For important data, measures such as encryption should be taken to prevent data leaks due to copying of files, theft, etc.		Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.

O111	V. Operational Guidelines	Use of cloud services	O111 Take measures to prevent the leakage of data on cloud service contract expiry.	To protect confidential information and prevent fraud, measures should be taken so that data does not leak from systems and equipment, etc. when the cloud service contract expires.		Cloud Platform customers own their data, not Google. The data that customers put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that Google will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
O112	V. Operational Guidelines	Use of cloud services	O112 Make preparations to conduct on-site audits and monitoring of cloud service providers.	The effectiveness of risk management systems, etc., needs to be confirmed for cloud service providers, since they are not easily managed directly with internal controls.		Google is certified to the ISO27001 Standard, which regulates "Independent Review of Information Security" (ISO 27001:2013, Annex A.18.2.1). In addition, Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Google conducts a number of audits to provide 3rd party validation of our control environment and provides validation of audits to customers, as needed. To review our current list of 3rd party compliance audits, please see the following pages: https://cloud.google.com/security/compliance https://G Suite.google.com/learn-more/compliance-google-apps.html
O113	V. Operational Guidelines	Preparing countermeasures against cyber attacks	O113 Prepare countermeasures against cyber attacks.	Since cyber attack methods have become increasingly advanced and sophisticated, preparations of countermeasures against cyber attacks need to be reviewed to keep up with this advance and sophistication of methods.		Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" ISO 27001:2013, (Annex A. 12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.

Technical						
Item No.	**Major Item**	**Medium Item**	**Minor Item**	**Concept of applicable location**		**Google Response**
T1	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Protection against hardware failure)	T1 Perform preventive maintenance of hardware.	To prevent hardware failure, perform preventive maintenance of hardware regularly or when necessary depending on the characteristics or importance of the devices.		Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (Annex A.11.2.4). Google's infrastructure utilizes container technology, and handles device failures flexible and seamlessly. It monitors malfunctioning devices constantly, and continues service even when problems are detected by transmitting data to other devices.

T2	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Protection against hardware failure)	T2 Provide a standby for a main unit.	Provide a standby to quickly handle a failure of an important main unit.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T3	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Protection against hardware failure)	T3 Provide standbys for peripherals.	To quickly handle failures of peripherals, provide standbys or substitute functions for important peripherals.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T4	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Protection against hardware failure)	T4 Provide standbys for communications devices.	To quickly handle failures in communications devices, provide standbys for important communications devices.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

T5	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Protection against hardware failure)	T5 Provide backup lines.	To quickly handle line failures, it is recommended that backup lines be provided for important lines.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T6	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Protection against hardware failure)	T6 Provide a standby for a terminal related device.	To quickly handle a failure in a terminal related device, provide a standby or a substitute function for it.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T7	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T7 For system development planning, check for proper consistency with medium- and long-term planning and obtain proper approvals.	For improving reliability of entire computer systems, system development plan should be consistent with medium- to long-term system plans, based on internal and external technology surveys, and approved by the development managers (heads of departments responsible for systems design and development).		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
T8	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T8 Include necessary security functions.	To ensure security measures, required security functions should be defined in the system-planning stage.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.

T9	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T9 Software quality should be assured at the design stage.	In order to improve software reliability at the design stage, the requirements of development should be defined, and software quality should be assured by consideration of reliability design and standardization of design work.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
T10	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T10 Ensure the quality of software in the phase of program development.	To improve the reliability of software in the phase of program development, programs should be developed in accordance with the program specifications, and the program development process should be standardized and automated to ensure the quality of software.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
T11	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T11 Ensure the quality of software in the phase of testing.	To improve the reliability of software in the phase of testing, ensure the quality of software by developing testing schedules, establishing testing environments and systems, utilizing test supporting capabilities, and controlling various involved factors in the phase of testing.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
T12	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T12 Ensure the reliability of software in consideration of program distribution.	To ensure the reliability of software during the distribution, it is essential to check for proper compatibility of software with the operating environments in the destinations of distribution and also to complete checking for viruses.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
T13	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality in development phase)	T13 Ensure the quality of package software when installed.	To ensure the quality of package software, fully check the incorporated features and proper compatibility with the own existing systems.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
T14	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality at the maintenance stage)	T14 Ensure the correctness of routined change operation.	To ensure the correctness of routined change operations such as new construction of a branch office and additional installation of devices, streamlining efforts and other required measures should be implemented for the change operations.		Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
T15	VI. Technical Guidelines I. Measures to improve hardware reliability	Measure to improve hardware reliability (Measures to improve quality at the maintenance stage)	T15 Ensure that the quality of software is maintained even after changing or adding any functions.	To ensure that the quality of software is maintained even after any functions are changed or added, apply quality improvement programs similar to those applied in the phase of development.		Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
T16	VI. Technical Guidelines I. Measures to improve hardware reliability	Measures to improve operational reliability (Measures to improve operational reliability)	T16 Automate and simplify operations.	To enhance the reliability of operations, it is recommended that operations be automated and simplified.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.

T17	VI. Technical Guidelines I. Measures to improve hardware reliability	Measures to improve operational reliability (Measures to improve operational reliability)	T17 Reinforce the functions of checking operations.	To prevent errors in operations, reinforce the checking functions.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
T18	VI. Technical Guidelines I. Measures to improve hardware reliability	Measures to improve operational reliability (Measures to improve operational reliability)	T18 Reinforce the functions of monitoring and controlling loaded conditions.	To ensure the stable operation of computer systems, reinforce the functions of monitoring the loaded conditions so that the performance and capacity limits of individual resources are not exceeded, and controlling the loaded conditions as needed.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
T19	VI. Technical Guidelines I. Measures to improve hardware reliability	Measures to improve operational reliability (Measures to improve operational reliability)	T19 Provide a remote control function for CD/ATM, etc.	For stable operation of CD/ATM in unmanned branches, provide the function of centrally monitoring their operational conditions and performing remote control as required.		Responsibility for validation of remote control functions for CD/ATM rests with the customer.
T20	VI. Technical Guidelines I. Measures to improve hardware reliability	Early failure detection and recovery (Early detection of failures)	T20 Provide the function of monitoring the operational conditions of a system.	To detect a failure at an early stage and to recover from it, provide the function of monitoring the operational conditions of a computer system (running, stopping and errors).		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
T21	VI. Technical Guidelines I. Measures to improve hardware reliability	Early failure detection and recovery (Early detection of failures)	T21 Provide the functions of detecting any failures and isolate the points of failure.	To facilitate quick failure recovery, provide the functions of accurately detecting any failures in the computer systems and problem determination.		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.

T22	VI. Technical Guidelines I. Measures to improve hardware reliability	Early failure detection and recovery (Early detection of failures)	T22 Provide the functions for reduction or shutdown and rearrangement of business operations in the event of failure.	To allow the system to keep running without shutting down the entire system in the event of failure even though some operations are interrupted, provide the functions of reducing the capabilities and rearranging the system.		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
T23	VI. Technical Guidelines I. Measures to improve hardware reliability	Early failure detection and recovery (Early detection of failures)	T23 Provide the functions of limiting transactions.	To minimize the impacts of file trouble or program errors, provide the functions of limiting transactions at the levels of file or account item.		Responsibility for minimizing errors at the account level is the responsibility of the customer.
T24	VI. Technical Guidelines I. Measures to improve hardware reliability	Early failure detection and recovery (Early detection of failures)	T24 Provide the recovery functions from failures.	Provide the required recovery functions for quick restoration of normal operation to systems and restarting of business operations in the event of failure.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.
T25	VI. Technical Guidelines I. Measures to improve hardware reliability	Disaster countermeasures (Backup centers)	T25 Establishment of backup centers.	For the case of a functional disorder of computer centers in disasters, it is recommended that backup centers be established in consideration of the priority of business operation.		Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.

T26	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data leakage)	T26 Take measures not to have personal identification numbers and passwords known by others.	For the protection of personal identification numbers and passwords known by others.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
T27	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data leakage)	T27 Provide the function of identifying a called terminal.	To prevent erroneous connection when outputting to an automatic answering terminal through public networks, it is recommended to provide the function of identifying a called terminal if possible.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
T28	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data leakage)	T28 Take measures for the protection of stored data against disclosure.	For the protection against disclosure by copying of files or burglary, it is recommended to take measures such as encrypting of important data.		Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
T29	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data leakage)	T29 Take measures to prevent leakage of transmission data.	To prevent leakage of transmission data through wiretapping, it is recommended that important data be encrypted.		Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.

T30	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data destruction and falsification)	T30 Provide proper exclusive access control to files.	To prevent possible inconsistency in file contents, provide proper exclusive control to files.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
T31	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data destruction and falsification)	T31 Provide the function of controlling access to files.	To protect data from unauthorized access, provide the function of checking the file access authorization of programs.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
T32	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Prevention of data destruction and falsification)	T32 Reinforce the functions of detecting any defective data.	To prevent any defective data from loading into systems, reinforce the functions of detecting and eliminating any defective data.		Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
T33	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Detection measures)	T33 Take measures for the detection of tampered transmitting data.	In the transmission of important data, it is recommended that measures be taken for the detection of falsification.		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.
T34	VI. Technical Guidelines II. Security Violation Countermeasures	Data protection (Detection measures)	T34 Provide the functions of matching files.	To early detect any inconsistencies between files due to intentional or accidental acts, provide the functions of ensuring a match between ledgers, checklists, journals, and other files.		Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A. 12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.

T35	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Verify access authorization))	T35 Set up functions of personal identification.	For prevention of unauthorized use, it should be confirmed that, according to business and connecting methods, connections are with authentic terminals or with identified persons.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
T35-1	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Verify access authorization))	T35-1 Examine required security control measures for biometric authentication in consideration of characteristics of biometrics.	For implementation of biometric authentication, examine required security control measures, taking into account the recent technological trends and giving careful consideration to the characteristics of biometrics.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
T36	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Verify access authorization))	T36 Provide the function of preventing unauthorized use of IDs/	To prevent unauthorized access, provide the function of preventing unauthorized use of IDs that are used to access systems, data, etc.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.

T37	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Verify access authorization))	T37 Manage access records.	For the management of access, records of access to systems and data should be obtained, which are kept as audit trail for a required time and checked periodically.		Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
T38	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Restrict scope of access))	T38 Provide the function of restricting transactions.	To prevent unauthorized access, provide the function of restricting transaction according to the type, location, and usage of devices, such as terminals, and media used in each transaction.		Responsibility for the prevention of unauthorized use resides with the customer.
T39	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Restrict scope of access))	T38 Provide the function of prohibiting transactions when an accident occurs.	To cope with accidents such as theft or loss of cards, passbooks, and seals, provide the function of prohibiting transactions through the account using the related medium when an accident occurs. Furthermore, to cope with accidents such as theft or loss at handheld terminals, provide a transaction prohibition function for each terminal.		Responsibility for the prevention of unauthorized use resides with the customer.
T40	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Unauthorized use and falsification countermeasures))	T40 Implement technical precautions against counterfeit card.	Proper technical precautions should be taken against counterfeit card to ensure protection against unauthorized use.		Customers are required to take appropriate precautions to prevent the use of counterfeit cards.
T41	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Unauthorized use and falsification countermeasures))	T41 Set up the protection of electronic value or take measures for detecting unauthorized use of it.	For countermeasures against copying electronic value and illicit actions such as violation of copyrights, the data-protective functions should be equipped, or the systems of detecting the occurrence of such actions should be set up.		Customers are required to take appropriate precautions to prevent the use of counterfeit cards.
T42	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Unauthorized use and falsification countermeasures))	T42 Provide the function of protecting cryptographic keys to devices and media that store electronic encryption keys, or software included with them.	To prevent the occurrence of illicit conducts resulting from the fact that a encryption key is known by others, provide the function of protecting encryption keys to devices, media, or software.		Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
T42-1	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Preventive measures (Unauthorized use and falsification countermeasures))	T42-1 Provide the function of preventing unauthorized sending/receiving e-mail, or browsing web sites, etc.	It is recommended that measures be taken to prevent unauthorized sending/receiving email, or browsing web sites, etc., for other than business purposes.		Customers are required to take appropriate precautions to prevent unauthorized browsing.

T43	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Restriction of access from external networks)	T43 Set up functions to protection against unauthorized access from external networks.	For the protection against unauthorized access, preventive measures against unauthorized access should be taken at the connective point with external networks (open networks, remote access, etc.) in the systems that handle important data and programs.		Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T44	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Restriction of access from external networks)	T44 Minimize connected devices that can be accessed from external networks.	To prevent intrusion into a computer system by means of unauthorized access, minimize communication routes and communications-related devices that can be accessed from outside, and do not connect unnecessary devices.		Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T45	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Detection measures)	T45 Provide the function of monitoring unauthorized access.	To detect unauthorized access at an early stage, provide the function of monitoring access errors and unauthorized access.		Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T46	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Detection measures)	T46 Provide the functions of identifying any unusual transactions.	To prevent damages due to illicit transactions, proper functions should be incorporated and implemented for early identification of any unusual transactions.		Customers are required to configure parameters to identify transactional anomalies.

T47	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Detection measures)	T 47 Provide the functions of monitoring exceptional transactions.	For early detection of any unauthorized access, proper functions should be provided for monitoring of exceptional transactions.		Customers are required to configure parameters to identify transactional anomalies.
T48	VI. Technical Guidelines II. Security Violation Countermeasures	Prevention of unauthorized use (Responsive measures)	T48 Take measures for protection against unauthorized access and of recovering.	For the cases of detecting unauthorized access, it is recommended that definite measures be taken for preventing the expansion of unauthorized access, as well as definite procedures of recovery. In cases of detecting unauthorized access, irrespective of being damaged, measures for preventing the expansion of unauthorized access and for recovery should be taken. In addition, after the analysis of the cause of unauthorized access, measures for preventing recurrence should be taken.		Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T49	VI. Technical Guidelines II. Security Violation Countermeasures	Malicious program prevention (Protective measures)	T49 Take preventive measures against malicious programs such as computer viruses.	In development, maintenance, and operations, measures should be taken for the prevention of damages resulting from malicious programs such as computer viruses.		Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.
T50	VI. Technical Guidelines II. Security Violation Countermeasures	Malicious prevention (Detection measures)	T50 Take proper precautions to detect any computer viruses and other malicious programs.	To ensure and maintain the reliability of computer systems, proper precautions should be taken to detect any intruded or embedded computer viruses and other malicious programs.		Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.

T51	VI. Technical Guidelines II. Security Violation Countermeasures	Malicious program prevention (Recovery measures)	T51 Take measures for cases involving damage from malicious programs such as computer viruses.	To minimize damages resulting from malicious programs such as computer viruses, measures ranging from the detection to the recovery of systems should be taken.		Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.