Google Workspace

CYBER SAFE | CYBER ESSENTIALS

Google Workspace Security Companion Guide for Cyber Essentials

October 2023

Table of Contents

Introduction

Working towards the Cyber Essentials certification from the Cyber Security Agency of Singapore (CSA) is a first step towards enhancing your organisation's cyber resilience. Keeping your organisation cyber secure is a journey, requiring continuous evolution to adapt to today's ever-changing threat landscape. To help you get started on this journey, CSA has worked with cloud service providers such as Google to create a suite of support resources. These include:

Cyber Essentials Mark

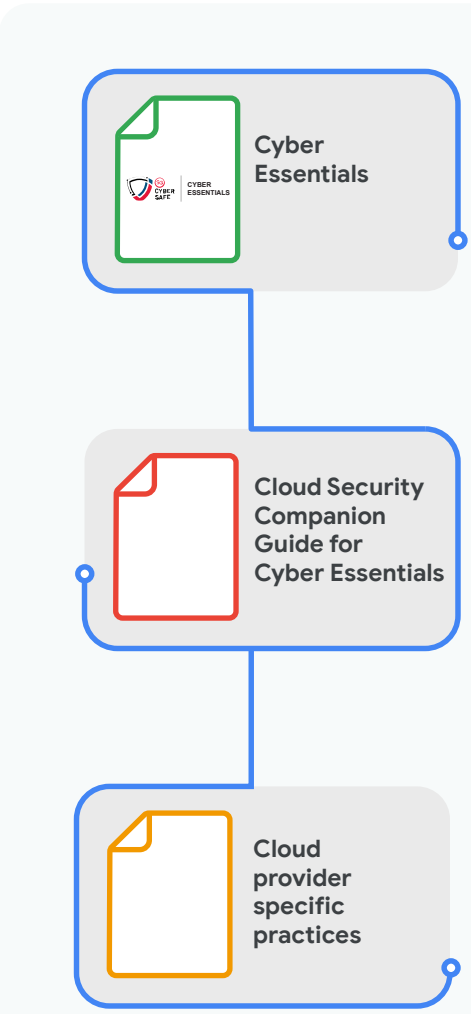
Developed by CSA and published as a national standard, the Cyber Essentials mark takes on a baseline control approach and is intended to protect organisations against the most common cyber attacks. It is part of a set of tiered cybersecurity standards that are designed to support the cybersecurity needs of a range of organisations.

Cloud Security Companion Guide for Cyber Essentials

Intended to serve as an implementation guide to accompany the Cyber Essentials mark, this document is targeted at cloud users implementing or preparing to implement the security measures in the Cyber Essentials mark. Since the Cyber Essentials mark is targeted at smaller or less digitalised organisations that are starting out in their cybersecurity journey, such as Small and Medium Enterprises (SMEs), this guide is scoped to target organisations that subscribe to the Software-as-a-Service (SaaS) cloud computing model, as this model tends to be more suited for small organisations.

SaaS Provider's Security Companion Guide for Cyber Essentials

These companion guides from individual SaaS providers offer more specific guidance on how their products' features map to the requirements outlined in the Cyber Essentials mark, providing recommendations to help their users maximise these product features, and an overview of the respective roles of the provider and the user.



This document, "Google Workspace Security Companion Guide for Cyber Essentials", falls under the third category. While we are proud to have built Google Workspace to be secure by default, securely using any cloud service is a shared responsibility between the cloud service provider and the user. To support you in obtaining or maintaining your Cyber Essentials mark, this document provides a mapping of the security features and tools in Google Workspace against the certification requirements of the Cyber Essentials mark. It explains how Google Workspace can support you in meeting each of the certification requirements and how you can best leverage Google Workspace. We have also included references to other materials that you may find helpful when exploring how to best use Google Workspace and its many security features. We are excited to support you on your journey as we keep the cyber space safer for everyone, together.

People

Equip employees with know-how to be the first line of defence

A.1.4(a) The organisation shall put in place cybersecurity awareness training for all employees to ensure that employees are aware of the security practices and behaviour expected of them. Organisations may meet this requirement in different ways, e.g., provide self-learning materials for employees or engaging external training providers.

Google Workspace User's Responsibility

Customers are responsible for determining what training to provide to employees. These decisions include whether and how to incorporate Google's materials on using Workspace securely, and adopt other security best practices.

Google's Responsibility

Customers using Google Workspace may decide to incorporate content from Google Cloud's Security Showcase into their training programs. These are on-demand topical video training sessions conducted by Google's product managers. Examples of relevant content include "What are the key security controls that I should have in place for Google Workspace?" and "How to protect your Gmail account from phishing and malware attacks".

Google's Safety Center also provides a set of general tools and tips to help customers stay safe online. This includes specific recommendations on steps that Google customers can take to protect their privacy and avoid scams.

More generally, Google customers may use information available on our free cybersecurity training or more advanced Google Cybersecurity Certificate, both via Coursera. Scholarships for the Google Cybersecurity Certificate are also available for eligible businesses.

A.1.4(b) Cyber hygiene practices and guidelines shall be developed for employees to adopt in their daily operations.

Google Workspace User's Responsibility

Customers are responsible for defining and drafting cyber hygiene best practices and may incorporate pre-existing recommendations on cyber hygiene from key software in use like Google Workspace.

Google's Responsibility

Customers may also refer to Google's checklists of best security practices, which are broken down based on business size.

A.1.4(c) The cyber hygiene practices and guidelines should include topics to mitigate cybersecurity incidents arising from the human factor as follows:

- Protect yourself from phishing;
- Set strong passphrase and protect them;
- Protect your corporate and/or personal devices (used for work);
- Report cybersecurity incidents;
- Handle and disclose business-critical data carefully; and
- Work onsite and remotely in a secure manner.

Google Workspace User's Responsibility

Customers are responsible for ensuring that their practices and guidelines address risks in their IT systems arising from inadvertent mistakes, including those in external cloud services like Google Workspace.

Google's Responsibility

Google's checklists of best security practices include recommendations designed to mitigate incidents caused by human error, including pointers on how to:

- Use Google resources to detect phishing,
- Set up strong passwords, and
- Limit access to sensitive files within Workspace.

Where available, customers can also rely on information about how to set up and manage our Data Loss Prevention (DLP) tool.

A.1.4(d) Where feasible, the training content should be differentiated based on the role of the employees:

- Senior management or business leaders – e.g., developing a cybersecurity culture/ mindset in the organisation or establishing a cybersecurity strategy or workplan.
- Employees – e.g., using strong passphrases and protecting the corporate and/or personal devices used for work.

Google Workspace User's Responsibility

Customers are responsible for determining whether role-based cybersecurity training is appropriate. Where deemed appropriate, customers are then responsible for determining what kinds of employees will receive what kind of cybersecurity training, as well as whether and how to incorporate training content made available through Google Workspace.

Google's Responsibility

Google's checklists of best security practices provide recommendations for a variety of users, including general employees and IT personnel.

A.1.4(e) **As good practice, such cybersecurity awareness initiatives should be conducted at least annually to refresh employees' awareness.**

Google Workspace User's Responsibility

Customers are responsible for scheduling at least annual cybersecurity refresher training. Customers are also responsible for deciding whether and how to account for their use of Google Workspace in those refresher training.

Google's Responsibility

Customers may refer to Google's resources noted above when conducting their refresher training.

Hardware and software

Know what hardware and software the organisation has and protect them

A.2.4(a) An up-to-date asset inventory of all the hardware and software assets shall be maintained in the organisation. Organisations may meet this requirement in different ways, e.g., use of spreadsheet or IT asset management software to maintain the IT asset inventory.

Google Workspace User's Responsibility

Customers are responsible for maintaining a current and comprehensive inventory of their own hardware (in their local environment) and software assets, including their cloud-based software assets like Google Workspace. Customers are also responsible for determining whether and how to use tools available through Google Workspace to support their inventory efforts.

Google's Responsibility

Google Workspace includes device inventory management that allows customers to easily see which devices (i.e., computers, laptops, mobile devices) are connected to or used to access Google Workspace. This inventory includes basic information about the device, such as operating systems level, browser level, and model. Customers may choose to extract this information and use it as part of their broader asset inventory management.

As customers build out these broader inventories that include other assets beyond those inventoried by Google Workspace, customers can also leverage Google Sheets or customise an AppSheet template for Equipment Inventory.

A.2.4(b) Hardware assets within the scope of certification may include servers, network devices, laptops and computers. If the scope of the certification includes hardware assets such as mobile devices and/or IoT devices:

Mobile devices

- Organisations should include company-issued mobile devices as part of its asset inventory, e.g., mobile phone and tablet.

IoT devices

- Organisations should include IoT devices used within the organisation as part of its asset inventory, e.g., Closed Circuit Television (CCTV), smart printer, smart television.

Google Workspace User's Responsibility

Customers are responsible for maintaining a current and comprehensive inventory of their own hardware assets in their local environment. Customers are also responsible for determining whether and how to use tools available through Google Workspace to support their inventory efforts.

Google's Responsibility

Please see A.2.4(a), which includes a description of how Google can help customers manage their inventory of assets.

A.2.4(c) The inventory list should contain details of the hardware assets where available as follows:

- Hardware name/model;
- Asset tag /serial number;
- Asset type;
- Asset location;
- Network address;
- Asset owner;
- Asset classification;
- Department;
- Approval/authorised date; and
- End of Support (EOS) date

Google Workspace User's Responsibility

Customers are responsible for maintaining relevant details in their inventories of their own hardware assets in their local environment. Customers are also responsible for determining whether and how to use tools available through Google Workspace to support their inventory efforts.

Google's Responsibility

Please see A.2.4(a), which includes a description of how Google can help customers identify relevant information about their hardware assets connecting to Workspace.

A.2.4(d) Software assets within the scope of certification may include software applications used by the organisation. If the scope of certification includes a cloud environment:

Cloud

- Organisation shall include what is hosted on the cloud instances, e.g., software and Operating System (OS).

Google Workspace User's Responsibility

Customers are responsible for accounting for their cloud-based software applications when populating their asset inventories, including completing information regarding their use of Google Workspace.

Google's Responsibility

N/A

A.2.4(e) The inventory list should contain the details of the software assets where available, as follows:

- Software name;
- Software publisher;
- Software version;
- Business purpose;
- Asset classification;
- Approval/authorised date; and
- EOS date.

Google Workspace User's Responsibility

Customers are responsible for maintaining relevant details in their inventories of software assets, including cloud-based assets like Google Workspace.

Google's Responsibility

N/A

A.2.4(f) As good practice, the hardware and software asset inventory list should be reviewed at least bi-annually (twice per year).

Google Workspace User's Responsibility

Customers are responsible for reviewing their hardware and software asset inventory lists at least twice per year, including inventory information related to their cloud services like Google Workspace.

Google's Responsibility

N/A

A.2.4(g) Hardware and software assets that are unauthorised or have reached their respective EOS shall be replaced.

Google Workspace User's Responsibility

Customers are responsible for replacing inappropriate assets on their systems in their local environment, including any unauthorised subscriptions to Google Workspace.

Google's Responsibility

Customer instances of Google Workspace reach their EOS period at the end of their subscription period. As long as customers maintain an active subscription to Google Workspace, their instance will not reach EOS.

A.2.4(h) In the event of any continued use of EOS assets, the organisation shall assess and understand the risk, obtain approval from senior management, and monitor it until the asset is replaced.

Google Workspace User's Responsibility

Customers are responsible for managing the risk of using their EOS assets in their local environment.

Google's Responsibility

N/A

A.2.4(i) An authorisation process shall be developed to onboard new hardware and software into the organisation. Organisations may meet this requirement in different ways, e.g., email approval from senior management, ensuring that new hardware and software come from official or trusted sources, performing malware scans to verify that the asset is clean and maintaining asset whitelisting/blacklisting.

Google Workspace User's Responsibility

Customers are responsible for determining and implementing an authorisation process for new hardware (in their local environment) and software, including cloud-based services like Google Workspace.

Google's Responsibility

N/A

A.2.4(j) The date of authorisation of software and hardware shall be keyed into the asset inventory list after obtaining the relevant dispensation, e.g., obtaining email approval or through the use of an approval form.

Google Workspace User's Responsibility

Customers are responsible for recording information about the authorisation of their hardware (in their local environment) and software, including cloud-based services like Google Workspace.

Google's Responsibility

N/A

A.2.4(k) Software and hardware without approval dates shall be removed.

Google Workspace User's Responsibility

Customers are responsible for identifying and removing unapproved hardware (in their local environment) and software, including cloud-based services like Google Workspace.

Google's Responsibility

N/A

A.2.4(l) Before disposing of any hardware asset, the organisation shall ensure that all confidential information have been deleted, e.g., encrypting hard disk before reformatting and overwriting it.

Google Workspace User's Responsibility

Customers are responsible for wiping sensitive information from their hardware assets before disposal, including determining whether and how to use Google Workspace tools like Endpoint Management to do so.

Google's Responsibility

When customers delete their data from Google Workspace, we delete the data from our systems within 180 days.

Google Workspace also includes the Endpoint Management security feature that logs and can block access to Workspace from any Windows, MacOS, Chrome OS, or Linux device. This feature also allows customers to wipe Workspace accounts from these devices.

A.2.4(m) **The organisation should carry out steps to ensure that the assets are disposed of securely and completely, e.g., destroy the hard disks physically or engage disk shredding services.**

Google Workspace User's Responsibility

Customers are responsible for securely disposing of all physical assets in their local environment over which they have control, such as external hard drives used to backup information managed in Google Workspace.

Google's Responsibility

Google uses barcodes and asset tags to meticulously track the location and status of all equipment within our data centres from acquisition and installation to retirement and destruction. We have also implemented metal detectors and video surveillance to help make sure no equipment leaves the data centre floor without authorisation.

Each data centre adheres to a strict disposal policy. When a hard drive is retired, authorised individuals verify that the disk is erased, writing zeros to the drive and performing a multiple-step verification process to ensure it contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. This physical destruction is a multistage 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.

Data

Know what data the organisation has, where they are, and secure the data

A.3.4(a) The organisation shall identify and maintain an inventory of business-critical data in the organisation. Organisations may meet this requirement in different ways, e.g., using spreadsheet or asset inventory software. The inventory list shall contain details of the data as follows:

- Description;
- Data classification and/or sensitivity;
- Location; and
- Retention period.

Google Workspace User's Responsibility

Customers are responsible for vetting and maintaining their inventories of business-critical data, as well as determining whether and how to use Google Workspace's Drive Label and Vault features to support their data inventory efforts.

Google's Responsibility

Customers can use Drive Labels to organise, find, and apply policies to items in Drive, Docs, Sheets, and Slides. Drive Labels are useful for many common scenarios, including:

- **Classifying content to follow an information governance strategy**: Drive Labels can be applied consistently across the entire organisation to identify sensitive content or content that requires special handling.
- **Applying policies to items**: Drive Labels can be used to ensure Drive content is managed throughout its lifecycle and adheres to the customer's record-keeping practices.
- **Curating and finding files faster**: Drive Labels increase searchability of the customer's Drive content.

In addition, Vault provides an information governance tool that can be used to retain, hold, search, and export Google Workspace data. This allows customers to:

- **Keep data for as long as they need it**: If the customer is required to preserve data for a set time, Vault can be configured to retain it. Data remains available via Vault even when employees delete it and empty their trash.
- **Remove data when they no longer need it**: If the customer is required to delete sensitive data after a set time, Vault can be configured to remove it from employees' accounts and purge it from all Google systems.

A.3.4(b) Review of the inventory list should be carried out at least annually, or whenever there is any change to the data captured by the organisation.

Google Workspace User's Responsibility

Customers are responsible for reviewing their data inventories at least once per year, including inventories that describe data maintained in Google Workspace.

Google's Responsibility

N/A

A.3.4(c) The organisation shall establish a process to protect its business-critical data, e.g., password protected documents, encryption of personal data (at rest) and/or emails.

Google Workspace User's Responsibility

Customers are responsible for determining how to best protect their business-critical data, including whether and how to leverage the security features built into Google Workspace.

Google's Responsibility

Customer data in Google Workspace is encrypted at rest and in transit, whether the data is on a disk, stored on backup media, moving over the Internet, or travelling between data centres.

Certain versions of Google Workspace also come equipped with a Security Center, which includes many features to protect customers and their data. These features include:

- **File Exposure**: Understand which files have been shared outside your domain and, where available, which shared files have triggered Data Loss Prevention (DLP) rules.
- **Authentication**: Find out how many messages do not meet your authentication standards (with additional and customisable "spoofing" features available for some customers).
- **Encryption**: Ensure that messages sent by your domain are encrypted using TLS.
- **Email Delivery**: See what percentage of incoming messages were accepted and whether whitelisting allowed suspicious messages to get delivered.
- **Spam and Malware Classification**: Analyse messages deemed to be spam, phishing, suspicious, or containing malware.
- **User Perception**: Evaluate whitelists by reviewing whether users have tagged delivered messages as spam or phishing.

A.3.4(d) There shall also be measures in place to prevent the employees from leaking confidential and/or sensitive data outside of the organisation, e.g., disabling USB ports.

Google Workspace User's Responsibility

Customers are responsible for determining which measures to implement to prevent employees from accidentally or deliberately leaking confidential or sensitive data, including whether and how to use the Data Loss Prevention feature within Google Workspace.

Google's Responsibility

Where available, customers can use Google Workspace's Data Loss Prevention (DLP) feature to create rules that control what content employees can share outside the organisation. DLP tools can help prevent employees from accidentally or deliberately sharing sensitive content and alert your IT team about any violations.

A.3.4(e) Before disposing of any paper-based (hard copy) media, the organisation shall carry out steps to ensure that those containing confidential and/or sensitive data have been securely shredded.

Google Workspace User's Responsibility

Customers are responsible for requiring that any hard copies of sensitive materials are appropriately shredded during disposal, including copies that are generated from data maintained in Google Workspace.

Google's Responsibility

N/A

Virus and malware protection

Protect from malicious software like viruses and malware

A.4.4(a) **Anti-malware solutions shall be used and installed in endpoints to detect attacks on the organisation's environment. Examples of endpoints include laptop computers, desktop computers, servers and virtual environments.**

Google Workspace User's Responsibility

Customers are responsible for deploying anti-malware solutions to the endpoints in their local environment, including determining whether and how to use the anti-malware features offered in their cloud environments like Google Workspace.

Google's Responsibility

The cloud infrastructure provider is typically responsible for the malware protection of the underlying cloud infrastructure.

Google Workspace provides customers with phishing and spam protection that blocks more than 99.9% of attacks before they can happen. Customers can adjust their Workspace settings to choose how to protect themselves against phishing and harmful software (malware), such as by moving suspicious content to the Spam folder or leaving it in the spam with a warning.

In addition, with advanced security settings, customers can protect against suspicious attachments and scripts from untrusted senders, identify links behind short URLs, scan linked images for malicious content, and protect against spoofing a domain name or employee names.

In addition to the Security Center discussed above in A.3, Workspace has a built-in Alert Center, which provides a comprehensive view of critical security alerts, notifications, and actions across all Google Workspace users and applications. The Alert Center also has the capability to allow for real-time action if suspicious activity is detected, including malware. It is integrated with VirusTotal, which provides crowdsourced threat intelligence from the broader security community to better understand any suspicious activity.

A.4.4(b) **Virus and malware scans shall be carried out to detect possible cyber attacks. Where feasible, scans should always be automated and remain active to provide constant protection.**

Google Workspace User's Responsibility

Customers are responsible for scanning the IT systems in their own local environment for viruses and malware.

Google's Responsibility

Please see A.4.4(a), which includes a description of how Google protects customers from phishing and spam, including those containing viruses and malware.

A.4.4(c) **Organisations shall enable auto-updates or configure the anti-malware solution to update signature files or equivalent (e.g., non-signature based machine learning solutions) to detect new malware. Where possible, these updates should take place at least daily to stay protected from the latest malware.**

Google Workspace User's Responsibility

Customers are responsible for enabling auto-updates and configuring their anti-malware solutions.

Google's Responsibility

N/A

A.4.4(d) **Anti-malware solution shall be configured to automatically scan the files upon access. This includes files and attachments downloaded from the Internet through the web browser or email and external sources such as from portable USB drives.**

Google Workspace User's Responsibility

Customers are responsible for scanning files before accessing them. Customers are also responsible for determining whether and how to use the anti-malware features offered in their cloud environments, like Google Workspace.

Google's Responsibility

Advanced security settings within Google Workspace include the following features:

- Attachments: Protection against suspicious attachments and scripts from untrusted senders. Includes protection against attachments types that are uncommon for your domain—these can be used to spread malware.

  Gmail can scan or run attachments in a virtual environment called Security Sandbox. Attachments identified as threats can be placed in users' Spam folders or quarantined.

- Links and external images: Identify links behind short URLs, scan linked images for malicious content, and display a warning when you click links to untrusted domains.

A.4.4(e) If the scope of certification includes mobile devices, IoT devices, cloud environment or use of web browser/email:

Mobile devices

- Anti-malware solution should be installed and running on mobile devices.

IoT devices

- Anti-malware solution should be integrated with the IoT devices, e.g., CCTV, smart television, smart printers, digital door lock.

Cloud

- Anti-malware solution should be deployed on the cloud platform.

Web browser/email

- Only fully supported web browsers and email client software with security controls should be used.
- Anti-phishing and spam filtering tools should be established for the web browser/email client software.
- Web browsers and/or email plug-ins/extensions/add-ons that are not necessary should be disabled and/or removed.
- Web filtering should be deployed to protect the business from malicious sites, where feasible.

Google Workspace User's Responsibility

Customers are responsible for deploying appropriate anti-malware solutions on their mobile devices, IoT devices, cloud environments, and web browser and email systems. This includes procuring, enabling, and managing anti-malware features available within those devices and services, including cloud environments like Google Workspace.

Google's Responsibility

Please see A.4.4(a) and (d), which include descriptions of how Google protects customers from phishing and spam in Workspace, including those containing viruses and malware.

A.4.4(f) Firewalls shall be deployed or switched on to protect the network, systems, and endpoints such as laptops, desktops, servers, and virtual environments. In an environment where there is an organisation's network setup, a network perimeter firewall shall be configured to analyse and accept only authorised network traffic into the organisation's network. Examples can include packet filter, Domain Name System (DNS) firewall and application-level gateway firewall with rules to restrict and filter network traffic. Depending on the organisation's network setup, the firewall functionality may be integrated with other networking devices or be a standalone device.

Google Workspace User's Responsibility

Customers are responsible for identifying and implementing a firewall structure in their local environment that is appropriate for their operations, including assessing firewall features and recommended settings available through cloud service providers like Google Workspace.

Google's Responsibility

Customers using Google Workspace may wish to refer to the service-specific requirements and recommendations for best practices about our firewall settings.

In addition, Context-Aware Access can be used to create granular access control policies to applications based on attributes such as user identity, location, device security status, and IP address.

A.4.4(g) In an environment where there are endpoints connecting to the Internet and/or cloud-based applications, a software firewall (host-based firewall) should be configured and switched on for all the endpoints in the organisation where available, e.g., turning on the built-in software firewall feature included in most operating systems or anti-malware solutions.

Google Workspace User's Responsibility

Customers are responsible for deploying and managing firewalls across their own IT systems in their local environment.

Google's Responsibility

N/A

A.4.4(h) As good practice, firewall configurations and rules should ideally be reviewed and verified annually to protect the organisation's Internet-facing assets where applicable.

Google Workspace User's Responsibility

Customers are responsible for annually reviewing their firewall configurations and for determining whether and how to account for firewall features and recommended settings available through cloud service providers like Google Workspace during these reviews.

Google's Responsibility

Please see A.4.4(f), which includes references to best practices that Google makes available for firewall configurations.

A.4.4(i) If the scope of certification includes mobile and/or IoT devices:

Mobile devices

- It is recommended that firewalls should be installed and enabled on employees' mobile devices.

IoT devices

- It is recommended that firewalls should be configured and enabled on IoT devices where possible.

Google Workspace User's Responsibility

Customers are responsible for deploying and managing firewalls across their own IT systems in their local environment.

Google's Responsibility

N/A

A.4.4(j) The organisation shall ensure that its employees install/access only authorised software/ attachments within the organisation from official or trusted sources.

Google Workspace User's Responsibility

Customers are responsible for ensuring that their employees use only authorised and trusted resources in their environments, including within their cloud environments like Google Workspace.

Google's Responsibility

Please see A.4.4(d), which includes a description of how Google Workspace helps customers identify suspicious attachments.
Customers using Google Workspace may wish to refer to Google's Safety Center for some tips to stay safe and secure online.

Customers can also control which third-party and domain-owned apps can access sensitive Google Workspace data.

A.4.4(k) **The organisation shall ensure that employees are aware of the use of trusted network connections for accessing the organisation's data or business email, e.g., mobile hotspot, personal Wi-Fi, corporate Wi-Fi and Virtual Private Network (VPN).**

Google Workspace User's Responsibility

Customers are responsible for informing their employees about trusted connections to their systems, including to cloud environments like Google Workspace.

Google's Responsibility

N/A

A.4.4(l) **The organisation shall ensure that its employees are aware of the need to report any suspicious email or attachment to the IT team and/or senior management immediately.**

Google Workspace User's Responsibility

Customers are responsible for ensuring that their employees know when and how to report suspicious emails or attachments, including those identified within Google Workspace.

Google's Responsibility

N/A

Access control

Control access to the organisation's data and services

A.5.4(a) Account management shall be established to maintain and manage the inventory of accounts. The organisation may meet this in different ways, e.g., using of spreadsheets or exporting the list from software directory services.

Google Workspace User's Responsibility

Customers are responsible for managing and tracking their system account users, including through the tools available to manage Google Workspace user accounts

Google's Responsibility

Google Workspace provides a centralised dashboard for customers to easily add and manage users and their devices.

A.5.4(b) The account inventory list shall contain details for user, administrator, third-party, and service accounts not limited to the following:

- Name;
- Username;
- Department;
- Role/account type;
- Date of access created; and
- Last logon date.

Google Workspace User's Responsibility

Customers are responsible for vetting and maintaining their inventories of all user accounts (including special role-based accounts), as well as determining whether and how to use Google Workspace's Administrator Dashboard to support these account inventory efforts.

Google's Responsibility

Google Workspace's centralised dashboard includes basic information about users and their devices. Google Workspace also logs actions taken by Google staff when accessing user content. These can be viewed through Access Transparency logs.

A.5.4(c) The organisation shall have a process with the necessary approvals to grant and revoke access. The organisation may implement this in different ways, e.g., email approval or access request form. This shall be implemented when there are personnel changes such as onboarding of new staff or change of role(s) for employees. The following fields shall be captured as follows:

- Name;
- System to access;
- Department;
- Role/account type;
- From date; and
- To date.

Google Workspace User's Responsibility

Customers are responsible for approving user access to their environments, including cloud environments like Google Workspace.

Google's Responsibility

N/A

A.5.4(d) Access shall be managed to ensure employees can access only the information and systems required for their job role.

Google Workspace User's Responsibility

Customers are responsible for managing employee account accesses based on their job responsibilities, including through the tools available to manage Google Workspace user accounts.

Google's Responsibility

Google Workspace allows customers to limit what functions and accesses their users can have, including through customised administrator roles.

A.5.4(e) Accounts with access rights that are no longer required or have exceeded the requested date shall have their access disabled or removed from the system. Shared, duplicate, obsolete and invalid accounts shall be removed.

Google Workspace User's Responsibility

Customers are responsible for auditing user accounts, including Google Workspace accounts, to ensure that their use is still appropriate.

Google's Responsibility

Google Workspace allows customers to disable or remove specific users at their discretion.

A.5.4(f) **The administrator account shall only be accessed to perform administrator functions with approval from the senior management.**

Google Workspace User's Responsibility

Customers are responsible for ensuring that system administrator accounts are used only for administrative functions, including whether and how to configure their systems (including Google Workspace) to restrict administrator account activities.

Google's Responsibility

Please see A.5.4(d), which includes a description of how Google allows customers to manage and customise their administrator accounts.

Google Workspace audit logs can also be shared with Google Cloud to store, analyse, monitor, and provide alerts on Google Workspace data and administrator user access.

A.5.4(g) **Access shall be managed to ensure that third parties or contractors can access only the information and systems required for their job role. Such access shall be removed once they no longer require them.**

Google Workspace User's Responsibility

Customers are responsible for managing third-party and contractor account accesses based on their job responsibilities, including through the tools available to manage Google Workspace user accounts.

Google's Responsibility

Please see A.5.4(d) and (e), which include descriptions of how Google allows customers to customise access for specific users.

A.5.4(h) **Third parties or contractors working with sensitive information in the organisation shall sign a non-disclosure agreement form. The form should include disciplinary action(s) for failure to abide by the agreement.**

Google Workspace User's Responsibility

Customers are responsible for ensuring that their third-party or contracted resources accessing sensitive information are subject to appropriate non-disclosure agreements, regardless of whether that information is maintained on premises or in Google Workspace.

Google's Responsibility

N/A

A.5.4(i) Physical access control shall be enforced to allow only authorised employees/ contractors to access the organisation's IT assets and/or environment, e.g., use of cable lock to lock the workstations and card access door lock to authenticate and authorise entry.

Google Workspace User's Responsibility

Customers are responsible for securing their own physical space and assets in their local environment.

Google's Responsibility

N/A

A.5.4(j) As good practice, account reviews should be carried out at least quarterly or whenever there are changes to the account list, e.g., during onboarding and offboarding processes or organisation restructuring.

Google Workspace User's Responsibility

Customers are responsible for reviewing all user accounts, including Google Workspace accounts, on a quarterly basis and determining when out-of-cycle reviews are warranted.

Google's Responsibility

N/A

A.5.4(k) Dormant or inactive accounts which have been inactive for a prolonged period, e.g., sixty (60) days should be removed or disabled.

Google Workspace User's Responsibility

Customers are responsible for removing or disabling all inactive user accounts, including Google Workspace accounts.

Google's Responsibility

N/A

A.5.4(l) The organisation shall change all default passwords and replace them with a strong passphrase, e.g., it should be at least twelve (12) characters long and include upper case, lower case, and/or special characters.

Google Workspace User's Responsibility

Customers are responsible for setting strong password credentials in lockstep with activating devices and accounts, including for Google Workspace accounts..

Google's Responsibility

Customers can enforce password requirements in Google Workspace, as well as see which users' passwords are weak by monitoring their password strength.

A.5.4(m) User accounts shall be disabled and/or locked out after multiple failed login attempts, e.g., after ten (10) failed login attempts, 'throttling' the rate of attempts.

Google Workspace User's Responsibility

Customers are responsible for configuring their systems to disable or lockout predefined suspicious log-in attempts, including attempts to log into Google Workspace.

Google's Responsibility

Google Workspace automatically detects and suspends certain suspicious login attempts. Customers can also set up customised account locks for multiple failed login attempts

A.5.4(n) The account password shall be changed in the event of any suspected compromise.

Google Workspace User's Responsibility

Customers are responsible for ensuring that any passwords suspected of compromise are changed, including passwords to Google Workspace accounts.

Google's Responsibility

Google Workspace allows customers to push bulk password reset via the Admin Console.

A.5.4(o) **Where feasible, two-factor authentication (2FA) should be used for administrative access to important systems, such as an Internet- facing system containing sensitive or business-critical data. Organisations may implement this in different ways, e.g., use of an authenticator application on the mobile or one-time password (OTP) token.**

Google Workspace User's Responsibility

Customers are responsible for procuring the technology necessary to provide 2FA, as well as configuring that technology (including Google Workspace) to ensure that administrators must use 2FA to access their systems.

Google's Responsibility

Google Workspace runs on Google Cloud Identity to provide a unified identity, access, app, and endpoint management (IAM/EMM) platform with the following key features:

- **Multi-factor authentication (MFA)**: Helps protect user accounts and customer data with a wide variety of MFA verification methods, including push notifications, Google Authenticator, phishing-resistant Titan Security Keys, and Android or iOS device security keys.
- **Single sign-on (SSO)**: Enables employees to work from virtually anywhere, on any device, with single sign-on to thousands of pre-integrated apps, both in the cloud and on-premises.

A.5.4(p) **Where feasible, trusted software to manage passphrases should be used to aid employee passphrase management.**

Google Workspace User's Responsibility

Customers are responsible for identifying and deploying password management software to assist employees accessing their systems, including Google Workspace.

Google's Responsibility

N/A

Secure configuration

Use secure settings for the organisation's hardware and software

A.6.4(a) Security configurations shall be enforced for the assets including desktop computers, servers and routers. Organisations may meet this requirement in different ways, e.g., adopting industry recommendations and standards such as Center for Internet Security (CIS) benchmarks on configuration guidelines across multiple vendor products, running baseline security analyser and/or using system configuration scripts.

Google Workspace User's Responsibility

Customers are responsible for identifying and enforcing appropriate security configurations for their systems, including whether to enforce default or recommended configurations provided by software vendors like Google Workspace.

Google's Responsibility

The provider is responsible for the application-level configuration settings.

Google's Security Center offers security health recommendations, which allow users to stay ahead of threats with recommended security settings and customised advice on security best practices for content, communication, mobility and user security.

A.6.4(b) Weak or default configurations shall be avoided or updated before using them, e.g., changing default password and performing deep scanning with anti-malware solution instead of standard scan.

Google Workspace User's Responsibility

Customers are responsible for avoiding insecure configurations, including whether to enforce default or recommended configurations provided by software vendors like Google Workspace.

Google's Responsibility

Please see A.6.4(a), which includes a description of Google resources for recommended security configurations.

A.6.4(c) Insecure configurations and weak protocols shall be replaced or upgraded to address the associated vulnerabilities, e.g., using Hypertext Transfer Protocol Secure (HTTPS) over normal Hypertext Transfer Protocol (HTTP) to encrypt data communication and upgrading Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access 2/3 (WPA2/WPA3) to enhance the Wi-Fi security standards.

Google Workspace User's Responsibility

Customers are responsible for avoiding insecure protocols, including whether to enforce default or recommended configurations provided by software vendors like Google Workspace.

Google's Responsibility

Please see A.6.4(a), which includes a description of Google resources for recommended security configurations.

A.6.4(d) Features, services, or applications that are not in use shall be disabled or removed, e.g., disabling file sharing services, software macros and File Transfer Protocol (FTP) ports.

Google Workspace User's Responsibility

Customers are responsible for determining what system functionality is unnecessary and should thus be disabled, including functionality available in Google Workspace.

Google's Responsibility

Customers can control which users can access which services in Google Workspace.

A.6.4(e) Automatic connection to open networks and auto-run feature of non-essential programs (other than backup or anti-malware solution, etc.) shall be disabled.

Google Workspace User's Responsibility

Customers are responsible for configuring their IT systems to avoid automatic connections to open networks or non-essential auto-runs.

Google's Responsibility

N/A

A.6.4(f) Logging should also be enabled for software and hardware assets where feasible, e.g., system, events and security logs.

Google Workspace User's Responsibility

Customers are responsible for enabling and managing logging within their systems, including Google Workspace.

Google's Responsibility

Please see A.5.4(b) and (f), which include descriptions of Google Workspaces audit logging functionality.

A.6.4(g) As good practice, automatic lock/session log out should be enabled after fifteen (15) min of inactivity for the organisation's assets. These include user sessions on the laptop computer, server, non-mobile device, database, and administrator portal.

Google Workspace User's Responsibility

Customers are responsible for configuring their systems to lock assets after inactive user sessions.

Google's Responsibility

N/A

A.6.4(h) If the scope of certification includes mobile devices, IoT devices, and/or cloud environment:

Mobile devices – e.g., mobile phone, tablet

- Mobile devices should not be jail-broken or rooted.
- Mobile device passcodes should be enabled.
- Automatic mobile device locks should be activated after two (2) min of inactivity.
- Mobile applications should only be downloaded from official or trusted sources.

IoT devices

- Network hosting the IoT devices should be separated from the network containing the organisation's assets and data.
- Security features should be enabled on IoT devices, e.g., turning off device auto-discovery and Universal Plug and Play (UPnP).
- In selecting IoT devices, the organisation should use devices rated by the Cybersecurity Labelling Scheme (CLS) (where available).

Cloud

- Security logging and monitoring should be turned on for cloud visibility, e.g., history of Application Programming Interface (API) calls, change tracking and compliance.

Google Workspace User's Responsibility

Customers are responsible for managing and monitoring the use of their assets, including cloud environments like Google Workspace.

Google's Responsibility

N/A

Software updates

Update software on devices and systems

A.7.4(a) **The organisation shall prioritise the implementation of critical or important updates for operating systems and applications (e.g., security patches) to be applied as soon as possible.**

Google Workspace User's Responsibility

Customers are responsible for prioritising updates to their software where they have the ability to do so. Customers are not responsible for prioritising software updates within Google Workspace, which Google manages for all of its customers.

Google's Responsibility

Google's servers and their OS are designed for the sole purpose of providing Google services, which means that, unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, that can introduce vulnerabilities. Google's environment also relies on automated mechanisms to monitor and remediate destabilising events, receive notifications about incidents, and slow down potential network compromises before they become critical issues.

Changes to Google Workspace, APIs, and Developer Offerings are delivered as software releases. All environment changes, including security patches, are carefully managed through a formal change management process. This includes procedures for tracking, testing, approving, implementing, and validating changes.
Google also staffs dedicated on-call personnel and incident response teams to manage, respond to, and track critical and important updates, including security patches for known vulnerabilities or incidents. These teams are organised into formalised shifts and are responsible for helping resolve emergencies 24 x 7.

A.7.4(b) **The organisation should carry out compatibility tests on updates for operating system and applications before installing them.**

Google Workspace User's Responsibility

Customers are responsible for testing updates to their software where they have the ability to do so. Customers are not responsible for testing software updates within Google Workspace, which Google manages for all of its customers.

Google's Responsibility

Please see A.7.4(a), which includes a description of how Google tests all software changes before implementing them in Google Workspace.

A.7.4(c) The organisation should consider enabling automatic updates for critical operating system and application patches where feasible so that they can receive the latest updates.

Google Workspace User's Responsibility

Customers are responsible for testing enabling automatic updates where they have the ability to do so. Customers are not responsible for enabling automatic updates within Google Workspace, which Google manages for all of its customers.

Google's Responsibility

Google has authored automated systems to ensure servers run up-to-date versions of their software stacks (including security patches) to detect and diagnose hardware and software problems, and to remove machines from service if necessary.

A.7.4(d) If the scope of certification includes mobile devices, IoT devices, and/or cloud environment:

Mobile devices – e.g., mobile phone, tablet

- The organisation should ensure that updates and patches for mobile devices are only downloaded from trusted sources (e.g., official app store from the manufacturer).
- IoT devices
- The organisation should remove or replace any IoT devices (e.g., CCTV, printers) that are not receiving any software patches or updates.

Cloud

- The organisation should refer to the cloud shared responsibility model with its Cloud Service Provider (CSP). This will allow organisations to be aware of when the organisation is responsible for software updates and security patches, and when the CSP is responsible.
- The organisation should have visibility on the software updates and security patches done by its CSPs.
- The organisation should also have security requirements regarding software updates defined for its CSPs.

Google Workspace User's Responsibility

Customers are responsible for reviewing this matrix and the terms of their agreement with Google Workspace to understand their and Google's shared responsibility for updates.

Google's Responsibility

Customers may refer to this matrix for an overview of how they and Google Workspace share responsibility for updates.

Back up essential data

Back up the organisation's essential data and store them offline

A.8.4(a) **The organisation shall identify business-critical systems and those containing essential business information and perform backup. What needs to be backed up is guided by identifying what is needed for business recovery in the event of a cybersecurity incident. Examples of business-critical systems include stock-trading system, railway operating and control system. Examples of essential business information include financial data and business transactions.**

Google Workspace User's Responsibility

Customers are responsible for determining what information to maintain as backups separate from their IT systems, including what specific information should be separately backed up from Google Workspace.

Google's Responsibility

Google periodically backs up data within Google Workspace Core Services to support the availability of user entity data. Google also periodically performs "data restore" tests on a subset of this data to confirm its availability for recovery. Google does not consider the nature of its customers' information when performing these recovery backups, such as how important the information is to the customer.
Customers may wish to use third-party tools, such as Spin.AI, to backup specific information stored in Google Workspace. Google Workspace also offers the data export tool Takeout, which customers can schedule for automatic data exports every two months.

A.8.4(b) **The backups shall be performed on a regular basis, with the backup frequency aligned to the business requirements and how many days' worth of data the organisation can afford to lose.**

Google Workspace User's Responsibility

Customers are responsible for determining how frequently to perform backups, including backups of specific information from Google Workspace.

Google's Responsibility

Please see A.8.4(a), which includes a description of Google Workspace's periodic recovery backups.

A.8.4(c) For non-business-critical systems or non-essential information, the backups should still be performed but at/on a lower frequency/long term basis.

Google Workspace User's Responsibility

Customers are responsible for determining how frequently to perform backups of less critical information, including backups of specific information from Google Workspace.

Google's Responsibility

Please see A.8.4(a), which includes a description of Google Workspace's periodic recovery backups.

A.8.4(d) The backup process should be automated where feasible.

Google Workspace User's Responsibility

Customers are responsible for determining whether and how to perform automated backups, including backups of specific information from Google Workspace.

Google's Responsibility

Please see A.8.4(a), which includes a description of Google Workspace's automated recovery backups.

A.8.4(e) If the scope of certification includes cloud environment:

Cloud

- The organisation shall understand the role and responsibility between itself and the CSP in terms of data backup, e.g., cloud shared responsibility model, scope, and coverage of the cloud service.
- Data backup shall be carried out by the organisation, e.g., storing the backups in a hard disk drive, purchasing the backup services by the CSP, and adopting multiple clouds to be used as backups.

Google Workspace User's Responsibility

Customers are responsible for reviewing this matrix and the terms of their agreement with Google Workspace to understand their and Google's shared responsibility for backups.

Google's Responsibility

Customers may refer to this matrix for an overview of how they and Google Workspace share responsibility for backups.

A.8.4(f) If the scope of certification includes hardware assets such as mobile devices and/or IoT devices:

Mobile devices

- Essential business information stored in mobile phones should be auto backed up and transferred to a secondary mobile phone or secondary storage for backup, e.g., SMS conversations or contact of an important client.

IoT devices

- IoT devices containing the organisation's essential information should be backed up manually, where automatic backup is not available, e.g., sensors in farms to improve operational safety and efficiency, and in healthcare to monitor patients with greater precision to provide timely treatment.

Google Workspace User's Responsibility

Customers are responsible for determining what information stored in mobile and IoT devices are to be maintained as backups.

Google's Responsibility

N/A

A.8.4(g) All backups shall be protected from unauthorised access and be restricted to authorised personnel only. Backups should minimally be password-protected.

Google Workspace User's Responsibility

Customers are responsible for protecting their backups, including backups of specific information from Google Workspace.

Google's Responsibility

Google Workspace allows customers to control who uses Google Takeout. The option to use Takeout will appear only for those users who have been given specific permission to use it.

A.8.4(h) Backups shall be stored separately (i.e., offline) from the operating environment. Where feasible, backups should be stored offsite, e.g., separate physical location.

Google Workspace User's Responsibility

Customers are responsible for storing their backups offline, including backups of information from Google Workspace.

Google's Responsibility

Please see A.8.4(a), which includes a description of third-party and Google Workspace tools that customers can use to store backups offline.

A.8.4(i) **Frequent backups, such as daily or weekly backups, should be stored online to facilitate quick recovery, e.g., cloud backup storage.**

Google Workspace User's Responsibility

Customers are responsible for performing online backups of their information, including backups of specific information from Google Workspace. Customers are not responsible for conducting Google's automated and generic recovery backups.

Google's Responsibility

Please see A.8.4(a), which includes a description of Google Workspace's online recovery backups.

A.8.4(j) **Longer term backups, such as daily or weekly backups, shall be stored offline in an external secure storage location, e.g., password-protected USB flash drives, encrypted external hard disks and/or tape storage at an alternative office location.**

Google Workspace User's Responsibility

Customers are responsible for externally storing their longer term backups, including backups of specific information from Google Workspace.

Google's Responsibility

Please see A.8.4(a) , which includes a description of third-party and Google Workspace tools that customers can use to externally store longer term backups.

A.8.4(k) **As good practice, backups should be tested at least bi-annually, or more frequently, to ensure that business-critical systems and essential business information can be restored effectively.**

Google Workspace User's Responsibility

Customers are responsible for testing backups of their information, including backups of specific information from Google Workspace. Customers are not responsible for testing Google's automated and generic recovery backups.

Google's Responsibility

Please see A.8.4(a), which includes a description of Google Workspace's recovery backups.

Incident response

Be ready to detect, respond to, and recover from cybersecurity incidents

A.9.4(a) The organisation shall establish an up-to-date basic incident response plan to guide the organisation on how to respond to common cybersecurity incidents. Examples include phishing, data breach, ransomware. The plan shall contain details as follows:

- Clear roles and responsibilities of key personnel in the organisation involved in the incident response plan process.
- Procedures to detect, respond to, and recover from the common cybersecurity threat scenarios, e.g., phishing, ransomware, data breach.
- Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management).

Google Workspace User's Responsibility

Customers are responsible for implementing an incident response plan that reflects their unique operating considerations, which may include partnerships with and resources provided by cloud service providers like Google Workspace.

Google's Responsibility

Google Cloud's security and resilience framework helps ensure business continuity and protects against adverse cyber events by using a comprehensive suite of solutions for every phase of the security and resilience lifecycle.

With the protection of customer data as its highest priority, Google Workspace runs an industry-leading information security operation that combines stringent processes, a world-class team, and multi-layered information security and privacy infrastructure to manage any data incident.

In addition to data protection features that are available for customers to configure, Google also provides a thorough data protection implementation guide for its customers in this whitepaper. Google also makes its data incident response process available publicly, which can be referred to by customers when adopting their own practices.

4.9.4(b) The incident response plan shall be made aware to all employees in the organisation that have access to the organisation's IT assets and/or environment.

Google Workspace User's Responsibility

Customers are responsible for socialising their incident response plans with their employees, including whether and how to use collaborative resources like Google Workspace to store, label, and share their plans.

Google's Responsibility

N/A

A.9.4(c) The organisation should conduct post- incident review and incorporate learning points to strengthen and improve the incident response plan.

Google Workspace User's Responsibility

Customers are responsible for conducting post-incident reviews and incorporating lessons learned, including where those reviews or lessons relate to customers' use of Google Workspace.

Google's Responsibility

N/A

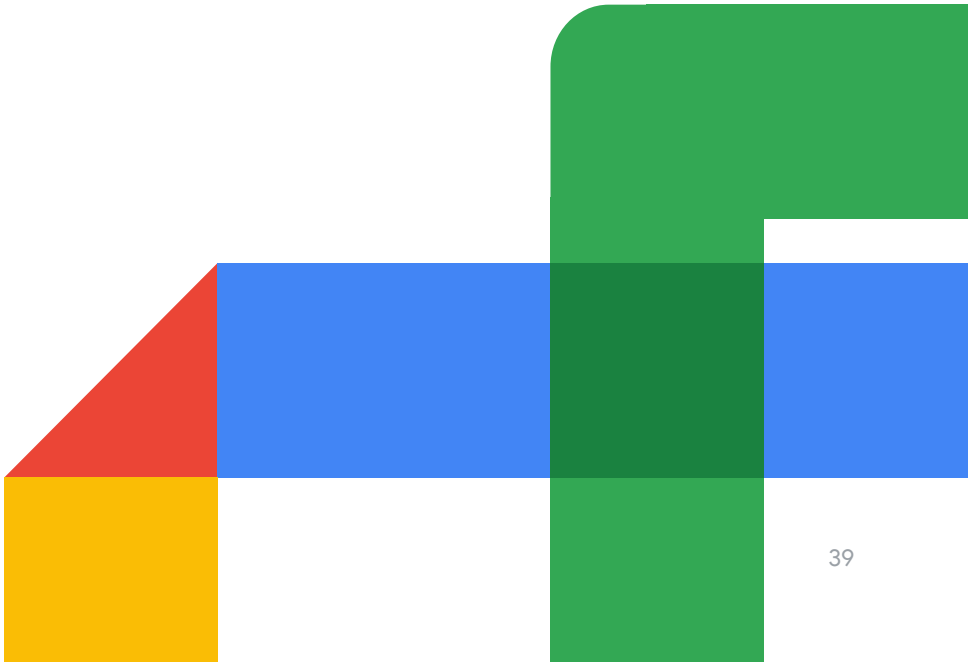
A.9.4(d) As good practice, the incident response plan should be reviewed at least annually.

Google Workspace User's Responsibility

Customers are responsible for reviewing their incident response plans at least annually, including where those plans relate to customers' use of Google Workspace.

Google's Responsibility

N/A



Google Workspace

SG CYBER SAFE | CYBER ESSENTIALS