YourIT!
Your Logo Goes Here

POPIA - Condition 7 - Security Safeguards

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Purpose

This policy applies to the workforce members of organisations that control or process personal information of Republic of South Africa citizens and residents.

Scope

POPIA applies to any organisation where the organisation is:
1) domiciled in the Republic; or
2) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

POPIA Section 1 - Definitions

POPIA - Condition 7 - Security Safeguards	Other Requirements
Section 1 Definitions	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

In this Act, unless the context indicates otherwise

"biometrics" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

"child" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;

"code of conduct" means a code of conduct issued in terms of Chapter 7;

"competent person" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

"consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"data subject" means the person to whom personal information relates;

"de-identify", in relation to personal information of a data subject, means to delete any information that
(a) identifies the data subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and "de-identified" has a corresponding meaning;

"direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of
(a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
(b) requesting the data subject to make a donation of any kind for any reason;

"electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"enforcement notice" means a notice issued in terms of section 95;

"filing system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"information matching programme" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"information officer" of, or in relation to, a
(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
(b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"Minister" means the Cabinet member responsible for the administration of justice;

"operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"person" means a natural person or a juristic person;

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to
(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

"prescribed" means prescribed by regulation or by a code of conduct;

"private body" means
(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
(b) a partnership which carries or has carried on any trade, business or profession; or
(c) any former or existing juristic person, but excludes a public body;

"processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

"professional legal adviser" means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

"public body" means

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
(b) any other functionary or institution when
(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
(ii) exercising a public power or performing a public function in terms of any legislation;

"public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"record" means any recorded information
(a) regardless of form or medium, including any of the following:
(i) Writing on any material;
(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
(iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
(iv) book, map, plan, graph or drawing;
(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
(b) in the possession or under the control of a responsible party;
(c) whether or not it was created by a responsible party; and
(d) regardless of when it came into existence;

"Regulator" means the Information Regulator established in terms of section 39;

"re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that
(a) identifies the data subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and re-identified" has a corresponding meaning;

"Republic" means the Republic of South Africa;

"responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"restriction" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"special personal information" means personal information as referred to in section 26;

"this Act" includes any regulation or code of conduct made under this Act; and

"unique identifier" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

Guidance
Understand the terms used in the POPIA regulations.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- POPIA.s1 - Definitions: The protection of data subjects in relation to the processing of personal information is a fundamental right. The POPIA Regulation applies to the processing of personal information of data subjects in the Republic of South Africa wholly or partly by automated means and to the processing other than by automated means of personal information which form part of any filing system or are intended to form part of any filing system. The POPIA regulations apply to the processing of personal information in the context of the activities of and establishment of a responsible party or an operator in the Republic of South Africa, regardless of whether the processing takes place in the Republic of South Africa or not.

  Procedure
  - Implement policies and procedures to comply with POPIA regulations as applicable
  - Bring in an independent expert to perform your risk assessment without any conflict of interest.

References

- The Protection of Personal Information Act, 2013 (Act 4 of 2013) - https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-act-2013-004.pdf
- The Information Regulator regulations relating to the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) - https://inforegulator.org.za/wp-content/uploads/2020/07/20181214-gg42110-rg10897-gon1383-POPIA-Regulations-1.pdf

POPIA Section 19(1)(a) - Security measures to prevent loss, damage, or unauthorized destruction

POPIA - Condition 7 - Security Safeguards	Other Requirements
Section 19(1)(a) Security measures to prevent loss, damage, or unauthorized destruction	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Security measures on integrity and confidentiality of personal information - Measures to prevent loss, damage, or unauthorized destruction:

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent
(a) loss of, damage to or unauthorised destruction of personal information

Guidance
In order to maintain security and to prevent processing in infringement of this Regulation, the responsible party or operator should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal information to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal information processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CIS1.1 - Establish and Maintain Detailed Enterprise Asset Inventory: Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

- CIS1.2 - Address Unauthorized Assets: Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

- CIS1.3 - Utilize an Active Discovery Tool: Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

- CIS1.4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory: Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

- CIS1.5 - Use a Passive Asset Discovery Tool: Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

- CIS2.1 - Establish and Maintain a Software Inventory: Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.

- CIS2.2 - Ensure Authorized Software is Currently Supported : Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfilment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

- CIS2.3 - Address Unauthorized Software: Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

- CIS2.4 - Utilize Automated Software Inventory Tools: Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

- CIS2.5 - Allowlist Authorized Software: Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

- CIS2.6 - Allowlist Authorized Libraries: Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

- CIS2.7 - Allowlist Authorized Scripts: Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

- CIS3.1 - Establish and Maintain a Data Management Process: Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.2 - Establish and Maintain a Data Inventory: Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

- CIS3.3 - Configure Data Access Control Lists: Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

- CIS3.4 - Enforce Data Retention: Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.

- CIS3.5 - Securely Dispose of Data: Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

- CIS3.6 - Encrypt Data on End-User Devices: Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

- CIS3.7 - Establish and Maintain a Data Classification Scheme: Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.8 - Document Data Flows: Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.9 - Encrypt Data on Removable Media: Encrypt data on removable media.

- CIS3.10 - Encrypt Sensitive Data in Transit: Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

- CIS3.11 - Encrypt Sensitive Data at Rest: Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

- CIS3.12 - Segment Data Processing and Storage Based on Sensitivity: Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

- CIS3.13 - Deploy a Data Loss Prevention Solution: Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.

- CIS3.14 - Log Sensitive Data Access: Log sensitive data access, including modification and disposal.

- CIS4.1 - Establish and Maintain a Secure Configuration Process: Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and

mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure: Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.3 - Configure Automatic Session Locking on Enterprise Assets: Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

- CIS4.4 - Implement and Manage a Firewall on Servers: Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

- CIS4.5 - Implement and Manage a Firewall on End-User Devices: Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

- CIS4.6 - Securely Manage Enterprise Assets and Software: Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

- CIS4.7 - Manage Default Accounts on Enterprise Assets and Software: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

- CIS4.8 - Uninstall or Disable Unnecessary Services on Enterprise Assets and Software: Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

- CIS4.9 - Configure Trusted DNS Servers on Enterprise Assets: Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

- CIS4.10 - Enforce Automatic Device Lockout on Portable End-User Devices: Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

- CIS4.11 - Enforce Remote Wipe Capability on Portable End-User Devices: Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

- CIS4.12 - Separate Enterprise Workspaces on Mobile End-User Devices: Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

- CIS5.1 - Establish and Maintain an Inventory of Accounts: Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- CIS5.2 - Use Unique Passwords: Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

- CIS5.3 - Disable Dormant Accounts: Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

- CIS5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- CIS5.5 - Establish and Maintain an Inventory of Service Accounts: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- CIS5.6 - Centralize Account Management: Centralize account management through a directory or identity service.

- CIS6.1 - Establish an Access Granting Process: Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

- CIS6.2 - Establish an Access Revoking Process: Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

- CIS6.3 - Require MFA for Externally-Exposed Applications: Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

- CIS6.4 - Require MFA for Remote Network Access: Require MFA for remote network access.

- CIS6.5 - Require MFA for Administrative Access: Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

- CIS6.6 - Establish and Maintain an Inventory of Authentication and Authorization Systems: Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

- CIS6.7 - Centralize Access Control: Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

- CIS6.8 - Define and Maintain Role-Based Access Control: Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control

reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

- CIS7.1 - Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- CIS7.2 - Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- CIS7.3 - Perform Automated Operating System Patch Management: Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- CIS7.4 - Perform Automated Application Patch Management: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- CIS7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- CIS7.6 - Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets: Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
- CIS7.7 - Remediate Detected Vulnerabilities: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- CIS8.1 - Establish and Maintain an Audit Log Management Process: Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- CIS8.2 - Collect Audit Logs: Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
- CIS8.3 - Ensure Adequate Audit Log Storage: Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.
- CIS8.4 - Standardize Time Synchronization: Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.
- CIS8.5 - Collect Detailed Audit Logs: Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
- CIS8.6 - Collect DNS Query Audit Logs: Collect DNS query audit logs on enterprise assets, where appropriate and supported.
- CIS8.7 - Collect URL Request Audit Logs: Collect URL request audit logs on enterprise assets, where appropriate and supported.

- CIS8.8 - Collect Command-Line Audit Logs: Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
- CIS8.9 - Centralize Audit Logs: Centralize, to the extent possible, audit log collection and retention across enterprise assets.
- CIS8.10 - Retain Audit Logs: Retain audit logs across enterprise assets for a minimum of 90 days.
- CIS8.11 - Conduct Audit Log Reviews: Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.
- CIS8.12 - Collect Service Provider Logs: Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.
- CIS9.1 - Ensure Use of Only Fully Supported Browsers and Email Clients: Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
- CIS9.2 - Use DNS Filtering Services: Use DNS filtering services on all enterprise assets to block access to known malicious domains.
- CIS9.3 - Maintain and Enforce Network-Based URL Filters: Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
- CIS9.4 - Restrict Unnecessary or Unauthorized Browser and Email Client Extensions: Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.
- CIS9.5 - Implement DMARC: To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.
- CIS9.6 - Block Unnecessary File Types: Block unnecessary file types attempting to enter the enterprise's email gateway.
- CIS9.7 - Deploy and Maintain Email Server Anti-Malware Protections: Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.
- CIS10.1 - Deploy and Maintain Anti-Malware Software: Deploy and maintain anti-malware software on all enterprise assets.
- CIS10.2 - Configure Automatic Anti-Malware Signature Updates: Configure automatic updates for anti-malware signature files on all enterprise assets.
- CIS10.3 - Disable Autorun and Autoplay for Removable Media: Disable autorun and autoplay auto-execute functionality for removable media.
- CIS10.4 - Configure Automatic Anti-Malware Scanning of Removable Media: Configure anti-malware software to automatically scan removable media.

- CIS10.5 - Enable Anti-Exploitation Features: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- CIS10.6 - Centrally Manage Anti-Malware Software: Centrally manage anti-malware software.

- CIS10.7 - Use Behavior-Based Anti-Malware Software: Use behavior-based anti-malware software.

- CIS11.1 - Establish and Maintain a Data Recovery Process : Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS11.2 - Perform Automated Backups : Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

- CIS11.3 - Protect Recovery Data: Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

- CIS11.4 - Establish and Maintain an Isolated Instance of Recovery Data : Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

- CIS11.5 - Test Data Recovery: Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

- CIS12.1 - Ensure Network Infrastructure is Up-to-Date: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

- CIS12.2 - Establish and Maintain a Secure Network Architecture: Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- CIS12.3 - Securely Manage Network Infrastructure: Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

- CIS12.4 - Establish and Maintain Architecture Diagram(s): Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA): Centralize network AAA.

- CIS12.6 - Use of Secure Network Management and Communication Protocols : Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

- CIS12.7 - Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure: Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

- CIS12.8 - Establish and Maintain Dedicated Computing Resources for All Administrative Work: Establish and maintain dedicated computing resources, either physically or logically

separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

- CIS13.1 - Centralize Security Event Alerting: Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

- CIS13.2 - Deploy a Host-Based Intrusion Detection Solution: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

- CIS13.3 - Deploy a Network Intrusion Detection Solution: Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

- CIS13.4 - Perform Traffic Filtering Between Network Segments: Perform traffic filtering between network segments, where appropriate.

- CIS13.5 - Manage Access Control for Remote Assets: Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

- CIS13.6 - Collect Network Traffic Flow Logs : Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

- CIS13.7 - Deploy a Host-Based Intrusion Prevention Solution: Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

- CIS13.8 - Deploy a Network Intrusion Prevention Solution: Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

- CIS13.9 - Deploy Port-Level Access Control: Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

- CIS13.10 - Perform Application Layer Filtering: Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

- CIS13.11 - Tune Security Event Alerting Thresholds: Tune security event alerting thresholds monthly, or more frequently.

- CIS14.1 - Establish and Maintain a Security Awareness Program: Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS14.2 - Train Workforce Members to Recognize Social Engineering Attacks: Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- CIS14.3 - Train Workforce Members on Authentication Best Practices: Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

- CIS14.4 - Train Workforce on Data Handling Best Practices: Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

- CIS14.5 - Train Workforce Members on Causes of Unintentional Data Exposure: Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

- CIS14.6 - Train Workforce Members on Recognizing and Reporting Security Incidents: Train workforce members to be able to recognize a potential incident and be able to report such an incident.

- CIS14.7 - Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates: Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

- CIS14.8 - Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks: Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

- CIS14.9 - Conduct Role-Specific Security Awareness and Skills Training: Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

- CIS15.1 - Establish and Maintain an Inventory of Service Providers: Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.2 - Establish and Maintain a Service Provider Management Policy: Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.3 - Classify Service Providers: Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.4 - Ensure Service Provider Contracts Include Security Requirements: Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security

requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

- CIS15.5 - Assess Service Providers: Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

- CIS15.6 - Monitor Service Providers: Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

- CIS15.7 - Securely Decommission Service Providers: Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

- CIS16.1 - Establish and Maintain a Secure Application Development Process: Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS16.2 - Establish and Maintain a Process to Accept and Address Software Vulnerabilities: Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

- CIS16.3 - Perform Root Cause Analysis on Security Vulnerabilities: Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

- CIS16.4 - Establish and Manage an Inventory of Third-Party Software Components: Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

- CIS16.5 - Use Up-to-Date and Trusted Third-Party Software Components: Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

- CIS16.6 - Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities: Establish and maintain a severity rating system and process for application

vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

- CIS16.7 - Use Standard Hardening Configuration Templates for Application Infrastructure: Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

- CIS16.8 - Separate Production and Non-Production Systems: Maintain separate environments for production and non-production systems.

- CIS16.9 - Train Developers in Application Security Concepts and Secure Coding: Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

- CIS16.10 - Apply Secure Design Principles in Application Architectures: Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

- CIS16.11 - Leverage Vetted Modules or Services for Application Security Components: Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

- CIS16.12 - Implement Code-Level Security Checks: Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

- CIS16.13 - Conduct Application Penetration Testing: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- CIS16.14 - Conduct Threat Modeling: Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

- CIS17.1 - Designate Personnel to Manage Incident Handling: Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.2 - Establish and Maintain Contact Information for Reporting Security Incidents: Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

- CIS17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents: Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.4 - Establish and Maintain an Incident Response Process: Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.5 - Assign Key Roles and Responsibilities: Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.6 - Define Mechanisms for Communicating During Incident Response: Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.7 - Conduct Routine Incident Response Exercises: Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

- CIS17.8 - Conduct Post-Incident Reviews: Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

- CIS17.9 - Establish and Maintain Security Incident Thresholds: Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS18.1 - Establish and Maintain a Penetration Testing Program: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls;

frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

- CIS18.2 - Perform Periodic External Penetration Tests: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

- CIS18.3 - Remediate Penetration Test Findings: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- CIS18.4 - Validate Security Measures: Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

- CIS18.5 - Perform Periodic Internal Penetration Tests: Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

- POPIA.s19 - Information System Security Plan: Develop, document, and periodically update information system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

  Procedure
  - Write a plan specifying the organisation security safeguards to be implemented by the organisation to protect personal information, protect other sensitive data, comply with regulations, and be available for an audit or investigation. Things change, requiring plan reviews and updates as necessary.

- POPIA.s19(1) - Physical Access Management: Manage and protect physical access to assets used to collect, transmit, process, and/or store personal information.

  Procedure
  - Use locks, guards, and other measures to block visitors and unauthorised staff members from getting to devices.

References

- The Protection of Personal Information Act, 2013 (Act 4 of 2013) - https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-act-2013-004.pdf
- The Information Regulator regulations relating to the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) - https://inforegulator.org.za/wp-content/uploads/2020/07/20181214-gg42110-rg10897-gon1383-POPIA-Regulations-1.pdf

POPIA Section 19(1)(b) - Security measures to prevent unlawful access or processing

POPIA - Condition 7 - Security Safeguards	Other Requirements
Section 19(1)(b) Security measures to prevent unlawful access or processing	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Security measures on integrity and confidentiality of personal information - Measures to prevent unlawful access or processing:

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent
(b) unlawful access to or processing of personal information.

Guidance
In order to maintain security and to prevent processing in infringement of this Regulation, the responsible party or operator should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal information to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal information processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CIS1.1 - Establish and Maintain Detailed Enterprise Asset Inventory: Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

- CIS1.2 - Address Unauthorized Assets: Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

- CIS1.3 - Utilize an Active Discovery Tool: Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

- CIS1.4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory: Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

- CIS1.5 - Use a Passive Asset Discovery Tool: Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

- CIS2.1 - Establish and Maintain a Software Inventory: Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.

- CIS2.2 - Ensure Authorized Software is Currently Supported : Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

- CIS2.3 - Address Unauthorized Software: Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

- CIS2.4 - Utilize Automated Software Inventory Tools: Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

- CIS2.5 - Allowlist Authorized Software: Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

- CIS2.6 - Allowlist Authorized Libraries: Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

- CIS2.7 - Allowlist Authorized Scripts: Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

- CIS3.1 - Establish and Maintain a Data Management Process: Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.2 - Establish and Maintain a Data Inventory: Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

- CIS3.3 - Configure Data Access Control Lists: Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

- CIS3.4 - Enforce Data Retention: Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.

- CIS3.5 - Securely Dispose of Data: Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

- CIS3.6 - Encrypt Data on End-User Devices: Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

- CIS3.7 - Establish and Maintain a Data Classification Scheme: Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.8 - Document Data Flows: Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.9 - Encrypt Data on Removable Media: Encrypt data on removable media.

- CIS3.10 - Encrypt Sensitive Data in Transit: Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

- CIS3.11 - Encrypt Sensitive Data at Rest: Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

- CIS3.12 - Segment Data Processing and Storage Based on Sensitivity: Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

- CIS3.13 - Deploy a Data Loss Prevention Solution: Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.

- CIS3.14 - Log Sensitive Data Access: Log sensitive data access, including modification and disposal.

- CIS4.1 - Establish and Maintain a Secure Configuration Process: Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and

mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure: Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.3 - Configure Automatic Session Locking on Enterprise Assets: Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

- CIS4.4 - Implement and Manage a Firewall on Servers: Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

- CIS4.5 - Implement and Manage a Firewall on End-User Devices: Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

- CIS4.6 - Securely Manage Enterprise Assets and Software: Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

- CIS4.7 - Manage Default Accounts on Enterprise Assets and Software: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

- CIS4.8 - Uninstall or Disable Unnecessary Services on Enterprise Assets and Software: Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

- CIS4.9 - Configure Trusted DNS Servers on Enterprise Assets: Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

- CIS4.10 - Enforce Automatic Device Lockout on Portable End-User Devices: Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

- CIS4.11 - Enforce Remote Wipe Capability on Portable End-User Devices: Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

- CIS4.12 - Separate Enterprise Workspaces on Mobile End-User Devices: Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

- CIS5.1 - Establish and Maintain an Inventory of Accounts: Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- CIS5.2 - Use Unique Passwords: Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

- CIS5.3 - Disable Dormant Accounts: Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

- CIS5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- CIS5.5 - Establish and Maintain an Inventory of Service Accounts: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- CIS5.6 - Centralize Account Management: Centralize account management through a directory or identity service.

- CIS6.1 - Establish an Access Granting Process: Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

- CIS6.2 - Establish an Access Revoking Process: Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

- CIS6.3 - Require MFA for Externally-Exposed Applications: Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

- CIS6.4 - Require MFA for Remote Network Access: Require MFA for remote network access.

- CIS6.5 - Require MFA for Administrative Access: Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

- CIS6.6 - Establish and Maintain an Inventory of Authentication and Authorization Systems: Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

- CIS6.7 - Centralize Access Control: Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

- CIS6.8 - Define and Maintain Role-Based Access Control: Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control

reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

- CIS7.1 - Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS7.2 - Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

- CIS7.3 - Perform Automated Operating System Patch Management: Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- CIS7.4 - Perform Automated Application Patch Management: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- CIS7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

- CIS7.6 - Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets: Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.

- CIS7.7 - Remediate Detected Vulnerabilities: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

- CIS8.1 - Establish and Maintain an Audit Log Management Process: Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS8.2 - Collect Audit Logs: Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

- CIS8.3 - Ensure Adequate Audit Log Storage: Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

- CIS8.4 - Standardize Time Synchronization: Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

- CIS8.5 - Collect Detailed Audit Logs: Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

- CIS8.6 - Collect DNS Query Audit Logs: Collect DNS query audit logs on enterprise assets, where appropriate and supported.

- CIS8.7 - Collect URL Request Audit Logs: Collect URL request audit logs on enterprise assets, where appropriate and supported.

- CIS8.8 - Collect Command-Line Audit Logs: Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
- CIS8.9 - Centralize Audit Logs: Centralize, to the extent possible, audit log collection and retention across enterprise assets.
- CIS8.10 - Retain Audit Logs: Retain audit logs across enterprise assets for a minimum of 90 days.
- CIS8.11 - Conduct Audit Log Reviews: Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.
- CIS8.12 - Collect Service Provider Logs: Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.
- CIS9.1 - Ensure Use of Only Fully Supported Browsers and Email Clients: Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
- CIS9.2 - Use DNS Filtering Services: Use DNS filtering services on all enterprise assets to block access to known malicious domains.
- CIS9.3 - Maintain and Enforce Network-Based URL Filters: Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
- CIS9.4 - Restrict Unnecessary or Unauthorized Browser and Email Client Extensions: Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.
- CIS9.5 - Implement DMARC: To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.
- CIS9.6 - Block Unnecessary File Types: Block unnecessary file types attempting to enter the enterprise's email gateway.
- CIS9.7 - Deploy and Maintain Email Server Anti-Malware Protections: Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.
- CIS10.1 - Deploy and Maintain Anti-Malware Software: Deploy and maintain anti-malware software on all enterprise assets.
- CIS10.2 - Configure Automatic Anti-Malware Signature Updates: Configure automatic updates for anti-malware signature files on all enterprise assets.
- CIS10.3 - Disable Autorun and Autoplay for Removable Media: Disable autorun and autoplay auto-execute functionality for removable media.
- CIS10.4 - Configure Automatic Anti-Malware Scanning of Removable Media: Configure anti-malware software to automatically scan removable media.

- CIS10.5 - Enable Anti-Exploitation Features: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- CIS10.6 - Centrally Manage Anti-Malware Software: Centrally manage anti-malware software.

- CIS10.7 - Use Behavior-Based Anti-Malware Software: Use behavior-based anti-malware software.

- CIS11.1 - Establish and Maintain a Data Recovery Process : Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS11.2 - Perform Automated Backups : Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

- CIS11.3 - Protect Recovery Data: Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

- CIS11.4 - Establish and Maintain an Isolated Instance of Recovery Data : Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

- CIS11.5 - Test Data Recovery: Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

- CIS12.1 - Ensure Network Infrastructure is Up-to-Date: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

- CIS12.2 - Establish and Maintain a Secure Network Architecture: Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- CIS12.3 - Securely Manage Network Infrastructure: Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

- CIS12.4 - Establish and Maintain Architecture Diagram(s): Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA): Centralize network AAA.

- CIS12.6 - Use of Secure Network Management and Communication Protocols : Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

- CIS12.7 - Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure: Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

- CIS12.8 - Establish and Maintain Dedicated Computing Resources for All Administrative Work: Establish and maintain dedicated computing resources, either physically or logically

separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

- CIS13.1 - Centralize Security Event Alerting: Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

- CIS13.2 - Deploy a Host-Based Intrusion Detection Solution: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

- CIS13.3 - Deploy a Network Intrusion Detection Solution: Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

- CIS13.4 - Perform Traffic Filtering Between Network Segments: Perform traffic filtering between network segments, where appropriate.

- CIS13.5 - Manage Access Control for Remote Assets: Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

- CIS13.6 - Collect Network Traffic Flow Logs : Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

- CIS13.7 - Deploy a Host-Based Intrusion Prevention Solution: Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

- CIS13.8 - Deploy a Network Intrusion Prevention Solution: Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

- CIS13.9 - Deploy Port-Level Access Control: Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

- CIS13.10 - Perform Application Layer Filtering: Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

- CIS13.11 - Tune Security Event Alerting Thresholds: Tune security event alerting thresholds monthly, or more frequently.

- CIS14.1 - Establish and Maintain a Security Awareness Program: Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS14.2 - Train Workforce Members to Recognize Social Engineering Attacks: Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- CIS14.3 - Train Workforce Members on Authentication Best Practices: Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

- CIS14.4 - Train Workforce on Data Handling Best Practices: Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

- CIS14.5 - Train Workforce Members on Causes of Unintentional Data Exposure: Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

- CIS14.6 - Train Workforce Members on Recognizing and Reporting Security Incidents: Train workforce members to be able to recognize a potential incident and be able to report such an incident.

- CIS14.7 - Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates: Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

- CIS14.8 - Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks: Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

- CIS14.9 - Conduct Role-Specific Security Awareness and Skills Training: Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

- CIS15.1 - Establish and Maintain an Inventory of Service Providers: Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.2 - Establish and Maintain a Service Provider Management Policy: Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.3 - Classify Service Providers: Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.4 - Ensure Service Provider Contracts Include Security Requirements: Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security

requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

- CIS15.5 - Assess Service Providers: Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

- CIS15.6 - Monitor Service Providers: Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

- CIS15.7 - Securely Decommission Service Providers: Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

- CIS16.1 - Establish and Maintain a Secure Application Development Process: Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS16.2 - Establish and Maintain a Process to Accept and Address Software Vulnerabilities: Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

- CIS16.3 - Perform Root Cause Analysis on Security Vulnerabilities: Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

- CIS16.4 - Establish and Manage an Inventory of Third-Party Software Components: Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

- CIS16.5 - Use Up-to-Date and Trusted Third-Party Software Components: Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

- CIS16.6 - Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities: Establish and maintain a severity rating system and process for application

vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

- CIS16.7 - Use Standard Hardening Configuration Templates for Application Infrastructure: Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

- CIS16.8 - Separate Production and Non-Production Systems: Maintain separate environments for production and non-production systems.

- CIS16.9 - Train Developers in Application Security Concepts and Secure Coding: Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

- CIS16.10 - Apply Secure Design Principles in Application Architectures: Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

- CIS16.11 - Leverage Vetted Modules or Services for Application Security Components: Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

- CIS16.12 - Implement Code-Level Security Checks: Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

- CIS16.13 - Conduct Application Penetration Testing: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- CIS16.14 - Conduct Threat Modeling: Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

- CIS17.1 - Designate Personnel to Manage Incident Handling: Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.2 - Establish and Maintain Contact Information for Reporting Security Incidents: Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

- CIS17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents: Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.4 - Establish and Maintain an Incident Response Process: Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.5 - Assign Key Roles and Responsibilities: Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.6 - Define Mechanisms for Communicating During Incident Response: Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.7 - Conduct Routine Incident Response Exercises: Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

- CIS17.8 - Conduct Post-Incident Reviews: Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

- CIS17.9 - Establish and Maintain Security Incident Thresholds: Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS18.1 - Establish and Maintain a Penetration Testing Program: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls;

frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

- CIS18.2 - Perform Periodic External Penetration Tests: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

- CIS18.3 - Remediate Penetration Test Findings: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- CIS18.4 - Validate Security Measures: Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

- CIS18.5 - Perform Periodic Internal Penetration Tests: Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

- POPIA.s19 - Information System Security Plan: Develop, document, and periodically update information system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

  Procedure
  - Write a plan specifying the organisation security safeguards to be implemented by the organisation to protect personal information, protect other sensitive data, comply with regulations, and be available for an audit or investigation. Things change, requiring plan reviews and updates as necessary.

- POPIA.s19(1) - Physical Access Management: Manage and protect physical access to assets used to collect, transmit, process, and/or store personal information.

  Procedure
  - Use locks, guards, and other measures to block visitors and unauthorised staff members from getting to devices.

References

- The Protection of Personal Information Act, 2013 (Act 4 of 2013) - https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-act-2013-004.pdf
- The Information Regulator regulations relating to the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) - https://inforegulator.org.za/wp-content/uploads/2020/07/20181214-gg42110-rg10897-gon1383-POPIA-Regulations-1.pdf

Truncated Sample Document