MORGANHILL

HAVE QUESTIONS?

Talk to a MorganHill Documentation Expert Today at 703-977-9044.

Listed below are selected excerpts from our industry leading ISMS security documentation available for download at shop.morganhillcg.com.

- ISMS 27002 - 5.3 - Segregation of Duties (SoD) Policy & Procedures
- ISMS 27002 - 5.11 - Return of Assets Policy & Procedures
- ISMS 27002 - 5.14 - Information Transfer Policy and Procedures
- ISMS 27002 - 6.1 - Employee and Contractor Screening Policy & Procedures
- ISMS 27002 - 7.7 - Clear Desk & Clear Screen Policy and Procedures
- ISMS 27002 - 8.19 - Software Installation Policy & Procedures
- ISMS 27002 - 8.20 - Network Security Policy & Procedures

DOWNLOAD NOW!

Insert Company Logo

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 5 - Organizational Controls

ISO 27002 Control Coverage: 5.3 – Segregation of Duties

Segregation of Duties (SoD) *Policy and Procedures*

Overview

The Segregation of Duties (SoD) policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Segregation of Duties policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Segregation of Duties policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Information Security Roles and Responsibilities | SoD – Information Systems

SoD for information systems is essential for helping ensure the safety and security of [company name]'s information systems. More specifically, SoD is an I.T. "best practice" that assists in ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s information system landscape. With increasing data security threats facing [company name], both internally and externally, it is vitally important to separate duties accordingly for ensuring no single user or group of users have complete control over any type of information security lifecycle.

Additionally, SoD applies to all environments within [company name], such as development, staging, and production, and is to include appropriate access controls for ensuring users have the minimum acceptable level of access necessary for performing his/her respective job function. As such, compensating controls are to be used as necessary when a complete separation of duties is not feasible.

Information Security Duties and User Departments & Users of Systems

Information security duties are to be segregated from the actual user department & user of information systems as this helps prevent fraud, error, and misuse of information systems. While user departments & user of systems are to provide meaningful input regarding information systems, it is not their responsibility to perform any relevant security duties. Specifically, security duties that should be segregated from user departments & users of systems are to include the following:

- Provisioning information systems.
- Establishing access rights and removing access for users assigned to information systems.
- Installing patches and other necessary security updates to information systems.
- De-commissioning and/or removing information systems from production.
- Changing configuration settings on information systems.
- Changing, modifying, disabling applications or other features currently in use.

Development, Testing and Production Environments

Separating development and testing environments from production environments is one of the most essential elements for SoD regarding information systems. Users that develop and/or test systems and applications are not to have access to production environments as unauthorized changes can create numerous issues that could ultimately harm [company name]'s information systems, such as un-approved changes to systems and files, along with possible failure of such systems. As such, separating development and test environments from production environments helps to ensure accidental and unauthorized changes that could affect the confidentiality, integrity, and availability (CIA) of [company name] information systems. The following mandates are to be implemented regarding SoD for development, testing and production environments:

- Development and testing environments access rights are to be separated from production environments.
- Development and testing personnel are not to have access to systems in production. When such SoD are not fully allowed, then compensating controls are to be implemented and enforced at all times.
- Different access control log-on initiatives are to be implemented to help reduce the risk of error, such as using different usernames and passwords for development and testing environments and for production environments.
- In such instances where a clear separation of personnel exists between development/testing environments and production environments, there is never to be a co-mingling of activities between such environments.

Development/Testing and Production Environment SoD Matrix

Name of System	Development/Testing Environment Description and SoD Controls	Production Environment and Description of SoD Controls
	Developers only have access to the online SaaS DEV environment, which is hosted at	Only production personnel have access to the online SaaS data analytics production

Online SaaS Data Analytics Portal	Amazon AWS, but on a completely different instance from the production environment, and on a completely different AWS account that is logically separated from the main AWS production environment, which has its own account.	environment, with developers not having any access whatsoever.
?	?	?
?	?	?

Development and I.T. Operations

Individuals responsible for developing, testing, and migrating information systems (i.e., applications and other supporting modules and I.T. systems) are to be segregated from I.T. operations. "I.T. Operations" are the personnel that perform the following duties:

- Data Entry
- Support Services
- I.T. Infrastructure and Operations

In essence, individuals using the information systems are those prohibited from developing, changing, and maintaining the information systems.

Database Administrator and I.T. Administrative Duties

Separating database administrator (DBA) duties from that of I.T. and platform specific administrative duties is essential for helping reduce fraud, error, and misuse of information systems. As such the following SoD are to be applied regarding separating duties between DBA functions and I.T. Administrative duties and functions:

- Revoke and/or remove external stored procedures permissions.
- Disallow I.T. administrators to have any type of DBA access rights credentials.
- Prohibit the use of mixed-code authentication to databases.
- Do not allow the database to be installed via local I.T. admin accounts.
- DBA level access to production databases is prohibited for any personnel that also have system software level access, or application developer access.
- Ensure that the following roles and responsibilities are effectively always segregated:
    - Database Administrator
    - Server Administrator
    - Backup Operator
    - Security Administrator

Segregation of Duties Best Practices

As necessary, and when applicable, authorized personnel at [company name] are to incorporate the following best practices regarding segregation of duties within the daily operational activities of the organization:

- *Clearly Define Roles and Responsibilities:* Clearly define job roles and responsibilities to ensure that there is a clear distinction between various functions within the organization.

- *Assign Tasks Based on Expertise:* Match tasks to employees' skills and qualifications to ensure that the right people are responsible for specific functions.
- *Implement Dual Authorization:* Require two or more individuals to authorize critical actions or decisions, reducing the risk of unauthorized activities.
- *Rotate Duties Periodically:* Periodically rotate employees' roles to minimize the risk of collusion and increase transparency.
- *Enforce Mandatory Vacation Periods:* Mandate that employees take vacations or leaves periodically, during which their responsibilities are temporarily assumed by someone else. This can help uncover potentially fraudulent activities during the absence.
- *Use Access Controls:* Implement strict access controls to limit individuals' ability to perform actions beyond their designated roles.
- *Review and Monitor Activity Logs:* Regularly review logs and audit trails to detect any suspicious or unauthorized activities.
- *Automate Processes:* Utilize automation and workflow management systems to enforce segregation of duties and ensure that critical tasks are handled by different individuals.
- *Create an Oversight Committee:* Establish an oversight committee to review and approve critical decisions independently.
- *Conduct Regular Risk Assessments:* Perform periodic risk assessments to identify potential vulnerabilities in the segregation of duties and make necessary adjustments.
- *Involve Management in Approval Processes:* Involve management in approving critical decisions or transactions to ensure accountability.
- *Educate Employees:* Educate employees about the importance of segregation of duties and the potential risks associated with not adhering to the principle.
- *Implement a Whistleblower Policy:* Establish a whistleblower policy that allows employees to report any concerns about potential violations of segregation of duties.
- *Continuous Improvement:* Regularly review and enhance the segregation of duties framework based on the organization's evolving needs and changing risk landscape.
- *Ensure Independence:* Avoid situations where an individual has the power to both initiate and approve transactions or decisions related to the same process.

Insert Company Logo

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 5 - Organizational Controls

ISO 27002 Control Coverage: 5.11 – Return of Assets

Return of Assets *Policy and Procedures*

Overview

The Return of Assets policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Return of Assets policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Return of Assets policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Scope of Assets

In terms of assets, [company name] is to ensure the proper return of the following items. This is not an all-inclusive list, rather, a starting point to use:

- Computer (Laptop)

- Printer, Scanner, Fax
- Cell Phone, Pager
- Portable Digital Assistant (PDA)
- USB Drives, External hard Drives, etc.
- Company Credit Card
- Access Devices-Keys
- Access Devices-Electronic Badges | Swipe Cards
- Furniture
- Pictures
- Uniforms
- Parking Permits

Company Owned Assets

All information systems owned, operated, maintained, and controlled by [company name] are deemed to be the sole property of the organization. As such, company assets in the possession of individuals (i.e., employees, contractors, etc.) are to be surrendered upon termination – either voluntarily or involuntary termination – from [company name]. Additionally, if an individual has legally acquired an asset from [company name], such as through a purchase – the asset is to be examined for ensuring no sensitive and unauthorized company and/or client data resides on the asset. If information is found, then the asset is to be seized with appropriate sanitization methods performed.

Assets Owned by Individuals

Likewise, if an individual is using his/her own asset, such as a laptop or any other type of computing system for conducting business activities, then the asset is to be examined by authorized I.T. personnel within [company name] prior to the individual's termination. As with [company name] owned assets, assets owned by individuals are to be examined for ensuring no sensitive and unauthorized company and/or client data resides on the asset. If information is found, then the asset is to be seized with appropriate sanitization methods performed.

Return of Assets Best Practices

As necessary, and when applicable, authorized personnel at [company name] are to incorporate the following best practices regarding the return of assets within the daily operational activities of the organization:

- *Comprehensive Inventory:* Maintain a detailed inventory list of all assets assigned to each employee.
- User Agreement: Have employees sign an agreement detailing their responsibilities regarding company-owned property upon onboarding.
- *Immediate Notice:* The terminated employee should be notified immediately and clearly about the need to return company assets.
- *Legal Consult:* Consult your HR and legal departments to ensure that the notification process is in compliance with labor laws.
- *Scheduled Handover:* Arrange a time and place for the terminated employee to return all company-owned property.
- *Supervised Retrieval:* Always conduct the retrieval process in the presence of a company representative, preferably from HR or IT, to ensure compliance and documentation.
- *Itemized List:* Provide an itemized list to the terminated employee of all items that need to be returned.
- *Physical Verification:* Physically check the returned items against the itemized list to ensure completeness and to assess condition.
- *Device Wiping:* Wipe all company data from returned devices in accordance with your company's data retention and destruction policies.

- *Access Revocation:* Immediately revoke access to company networks, databases, email, and other sensitive resources.
- *Receipt Acknowledgment:* Both parties should sign an acknowledgment receipt indicating that all items have been returned and are in acceptable condition.
- *Audit Trail:* Keep a detailed record of the returned items, their condition, and any actions taken (e.g., data wiping, refurbishing).
- *Reimbursement:* Process any necessary reimbursements for deposits or expense claims related to the returned property.
- *Damage Charges:* If any property is damaged, follow a pre-established process for assessing and collecting costs.
- *Legal Clearance:* Obtain clearance from the legal department confirming that all company-owned property has been returned and data has been secured.
- *Confidentiality Reminders:* Remind the terminated employee of any ongoing confidentiality or non-compete obligations.
- *Secure Storage:* Store the returned items securely until they can be re-assigned or disposed of.
- *Update Inventory:* Update your asset inventory list to reflect the returned items.

Insert Company Logo

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 5 - Organizational Controls

ISO 27002 Control Coverage: 5.14 – Information Transfer

Information Transfer *Policy and Procedures*

Overview

The Information Transfer policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Information Transfer policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Information Transfer policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Transfer of Information

Information being transferred using all types of communication facilities must be protected at all times. With growing cybersecurity threats, all personnel are to be aware of the organization's information transfer policies,

procedures, and processes. The goal when transferring information is to ensure the confidentiality, integrity, and availability (CIA) of the data being sent and/or received by [company name]. This in turn requires the use of numerous industry approved data transmission protocols, along with supporting software solutions that are to be used at all times.

From a procedures perspective, information transfer activities are to be done so with approved data transmission protocols, using approved systems. Depending on the type of data being sent, various protection methods are to be used, ranging from encryption to password protecting files, and other necessary mechanisms. Additionally, [company name] has in place numerous acceptable uses policies that guide users on various aspects of sending and receiving data. Furthermore, authorized personnel at [company name] are to configure a deploy network tools and solutions that aid and assist in such endeavors for the protection of information transfer. Together, these procedures help information from being intercepted, copied, modified, misrouted, and/or destroyed.

Protection Against Malware

[Company name] mail servers are to be configured will all necessary mail anti-malware solutions, such as antivirus and anti-spam, along with other essential utilities for effectively blocking and containing email born viruses and other malware threats. Specifically, all email communications and web browsing for webmail must be sent through the applicable email filtering systems for ensuring file extensions that are known to contain malware, such as .vbs, .dat, .exe, .pif. .scr, are blocked. Additionally, many commonly used file extensions can also contain malware, thus use caution at all times when opening, saving attachments, or forwarding them also.

Protection of Attachments

Attachments, which are often sent with emails, are to be protected if the information is deemed sensitive in nature. Please refer to [company name]'s data classification matrix to determine the classification of data and if the attachment needs to be protected. Two (2) methods are to be used for protecting attachments, either (1). Password protection, or (2). Encryption. All attachments, regardless of format (i.e., zip file, pdf, Microsoft Word, photos, etc.) must thus either be encrypted or password protected. Please refer to the actual tool or solution used for the relevant procedures.

Acceptable Use of Communication Facilities

The following guidelines, for which all personnel are to receive copies on and acknowledge, provide guidance and acceptable usage rights regarding [company name]'s communication facilities and related assets:

- Laptop Usage Policy and Procedures
- Information System Usage Policy and Procedures
- Internet Usage Policy and Procedures
- Software Usage Policy and Procedures

User Responsibilities

The following guidelines, for which all personnel are to receive copies on and acknowledge, provide guidance on specific unacceptable behavior, specifically, the following: defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.

- Laptop Usage Policy and Procedures
- Information System Usage Policy and Procedures
- Internet Usage Policy and Procedures
- Software Usage Policy and Procedures
- E-Mail Usage Policy and Procedures

Cryptographic Techniques

[Company name] is to utilize encryption standards as designated by the "Federal Information Processing Standards (FIPS), which consist of publicly announced standardization documentation developed by the U.S. government and issued by the National Institute for Standards and Technology (NIST). Specifically, **FIPS 140-2** | Security Requirements for Cryptographic Modules and **FIPS-197** | Advanced Encryption Standard (AES) form the basis of approved encryption standards and strengths for all products and protocols used by [company name] regarding confidentiality and integrity of data.

Other standards and best practices that provide encryption guidance, such as those advocated by the **The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**, are to be utilized also. The GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

Additionally, cryptographic protocols are to be utilized for data transmission activities over untrusted networks, which include, but are not limited to, the following:

- **IPSec:** Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet within the actual communication session.
- **TLS | SSL:** Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet utilizing both asymmetric and symmetric cryptography.
- **SSH:** Secure Shell (SSH) is a cryptographic network protocol for secure data communication between two networked computers that connect through a secure channel over an insecure network, a server and a client.

Cryptographic Protocol in Use	Description	Business Justification for Use
IPSec	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet within the actual communication session.	
TLS | SSL	Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet utilizing both asymmetric and symmetric cryptography.	
SSH	Secure Shell (SSH) is a cryptographic network protocol for secure data communication between two networked computers that connect through a secure channel over an insecure network, a server and a client.	
?		
?		
?		

Retention and Disposal Guidelines

Data retention and disposal guidelines are outlined specifically within [company name]'s **Protection of Records Policy and Procedures** which provides detailed information regarding as to the types of data kept and the relevant disposal techniques used.

Controls and Restrictions on Communication Facilities

The use of communications facilities must be made in accordance with one's roles and responsibilities at [company name]. As such, all personnel are to be aware of general best practices, which include, but are not limited to, the following:

- Limiting physical access only to areas where allowed.
- Limiting logical access only to systems allowed.
- Dressing and acting in an appropriate, professional manner at all times.
- Adhering to all stated employment requirements, acceptable usage policies, and more.

Appropriate Precautions

Ensuring the safety and security of confidential information is paramount, and as such, personnel are to never access systems for which they have not been given authorization to, never leaving information in public areas, along with employing other necessary best practices. The following guidelines, for which all personnel are to receive copies on and acknowledge, provide guidance and acceptable usage rights regarding [company name]'s regarding confidential information.

- Laptop Usage Policy and Procedures
- Information System Usage Policy and Procedures
- Internet Usage Policy and Procedures
- Software Usage Policy and Procedures
- E-Mail Usage Policy and Procedures

Answering Machines

Answering machines, if still in use, are never to store sensitive information, as it can be easily re-played and copied by an unauthorized individual. The same holds true for cellular voice mails, as such messages can also be re-played, even forwarded, to another cellular phone.

Facsimile Machines

Facsimile (fax) machines, if still in use, are to be safeguarded from the following security issues:

- Unauthorized access to built-in message stores to retrieve messages.
- Deliberate or accidental programming of machines to send messages to specific numbers.
- Sending documents and messages to the wrong number either by misdialing or using the wrong-stored number.

Insert Company Logo

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 6 – People Controls

ISO 27002 Control Coverage: 6.1 – Screening

Employee and Contractor Screening *Policy and Procedures*

Overview

The Employee and Contractor Screening policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Employee and Contractor Screening policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Employee and Contractor Screening policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Screening Measures

One of the most important initiatives [company name] can undertake for ensuring the best possible candidates become employees that ultimately provide long-term value to the company is by implementing proper screening

initiatives. Employees that do not meet stringent background checks are to be immediately disqualified from employment with [company name] – no exceptions. As such, the following screening initiatives are to be performed for all candidates and new hires seeking employment with [company name]:

- Character references from previous employers and/or other relevant individuals.
- Verification of prior employment.
- Verification of claimed academic achievement and professional qualifications, licensing, certifications, etc.
- Verification of one's actual identity.
- Where applicable, credit reviews are to be performed.
- Where applicable, criminal background checks are to be performed.
- Where applicable, drug tests are to be performed.

Upon being hired, if an individual is being given a specific role, duty, or function within the broader realm of information security, procedures are to be undertaken for ensuring the individual as the requisite skills for performing the job. If such job functions required the handling of sensitive information, then additional screening procedures are to be undertaken as necessary.

The aforementioned information is also to apply to contractors being used by [company name], thus authorized personnel at [company name] are to ensure such measures have been performed, and that proof can be provided as necessary.

Lastly, all employee screening initiatives are to be performed in accordance with prescribed laws and regulations, by authorized personnel, with all screening evidence collected, retained, and ultimately destroyed as required.

Screening Process – Direct Company Hire	Is Applicable Screening Process Performed? (Yes, No, or NA)	Description of Relevant Screening Process Performed for Employees	Responsible Party
Character References			
Verification of Prior Employment			
Verification of Academic Achievement			
Verification of Professional Qualifications. Licensing, and Certifications			
Verification of one's Actual Identity			
Credit Check			
Criminal Background Check			
Drug Test			
Other			

Contractor Screening			

Screening Process - Contractors	Is Applicable Screening Process Performed? (Yes, No, or NA)	Description of Relevant Screening Process Performed for Contractors and all other individuals designated as "non-employees".	Responsible Party
Character References			
Verification of Prior Employment			
Verification of Academic Achievement			
Verification of Professional Qualifications. Licensing, and Certifications			
Verification of one's Actual Identity			
Credit Check			
Criminal Background Check			
Drug Test			
Other			
Contractor Screening			

Note: The above-listed policies and best practices for **Screening** should also be documented within your organization's enterprise-wide H.R. policies. However, feel free to document your screening initiatives in the above referenced matrices if such policies do not exist.

Employee Screening Best Practices

As necessary, and when applicable, authorized personnel at [company name] are to incorporate the following best practices regarding employee screening within the daily operational activities of the organization:

- *Establish Clear Screening Policies:* Define comprehensive screening policies that outline the types of checks required for different roles, the criteria for disqualification, and the process for conducting screenings.
- *Adhere to Legal and Regulatory Standards:* Ensure that all screening practices align with applicable local, state, and federal laws, including anti-discrimination and privacy regulations.
- *Screen All Job Applicants:* Implement a consistent screening process for all job applicants to maintain fairness and avoid potential bias.
- *Tailor Screenings to Job Roles:* Customize screening requirements based on the specific responsibilities of each role. Some positions may require more rigorous checks than others.

- *Obtain Consent and Provide Disclosure:* Obtain written consent from applicants before conducting screenings and provide clear disclosure about the types of checks that will be performed.
- *Utilize Reputable Screening Providers:* Partner with reputable background screening providers that adhere to industry standards and can provide accurate and up-to-date information.
- *Check Criminal History:* Conduct criminal background checks to identify any potential criminal history that could impact the applicant's suitability for the role.
- *Verify Employment History:* Verify the accuracy of an applicant's employment history, including job titles, dates of employment, and roles held.
- *Confirm Educational Credentials:* Validate an applicant's educational credentials by checking with the educational institutions listed on their resume.
- *Assess Professional Licenses and Certifications:* Verify any professional licenses or certifications that are relevant to the job role, ensuring they are valid and in good standing.
- *Review Credit History (If Applicable):* Consider conducting credit checks for positions that involve financial responsibilities to assess an applicant's financial stability.
- *Conduct Social Media Checks (Within Legal Boundaries):* If relevant, review an applicant's social media presence, ensuring that the process adheres to privacy laws and regulations.
- *Check References:* Contact provided references to gather insights into an applicant's work ethic, skills, and professional demeanor.
- *Use Consistent Interview Questions:* Design consistent interview questions that help identify red flags and gather relevant information about an applicant's background.
- *Train Hiring Managers and HR Staff:* Provide training to those involved in the hiring process to ensure they understand the importance of screenings and how to interpret results.
- *Maintain Applicant Privacy:* Safeguard applicant information and ensure that only authorized personnel have access to screening results.
- *Ensure Fairness and Consistency:* Apply screening practices uniformly to all applicants to prevent discrimination or bias in the hiring process.
- *Keep Records Secure:* Maintain secure records of all screening results and related documentation, ensuring compliance with data protection regulations.
- *Communicate Screening Outcomes:* Clearly communicate the results of screenings to applicants, allowing them an opportunity to address any discrepancies or inaccuracies.
- *Review and Update Policies Regularly:* Periodically review and update screening policies to ensure they remain current and effective in addressing emerging concerns.
- *Provide Appeals Process:* Offer applicants an appeals process if they believe they were wrongly disqualified due to screening results.
- *Integrate Screening with Onboarding:* Seamlessly integrate screening results into the onboarding process to ensure a smooth transition for new hires.
- *Regularly Audit Screening Processes:* Conduct regular internal audits of the screening process to identify areas for improvement and ensure compliance.
- *Collaborate with Legal Experts:* Consult with legal experts or employment attorneys to ensure that screening practices align with legal requirements.
- *Promote Transparency with Employees:* Communicate the organization's screening policies and practices to current employees to foster transparency and trust.

Insert Company Logo

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 7 – Physical Controls

ISO 27002 Control Coverage: 7.7 – Clear Desk and Clear Screen

Clear Desk and Clear Screen *Policy and Procedures*

Overview

The Clear Desk and Clear Screen policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Clear Desk and Clear Screen policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Clear Desk and Clear Screen policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

General Awareness of One's Work Environment

Ensuring the safety and security of one's workspace environment requires a general awareness and knowledge of basic, yet essential, security best practices. Not leaving passwords on Post It Notes, securing sensitive documents in

a locked cabinet when not in use; these are just a few of the security requirements that all users are to be aware of regarding the security of one's workspace. While most security practices should be inherently known, it's also important that all users undergo annual security awareness training to gain additional knowledge on other subjects relating to the safety and security of one's workspace.

It's also important to note the following clear desk and clear screen requirements are to be in place wherever a user is working – at the office, at home, on the road. Keeping a "security first" mindset ultimately helps in ensuring the safety and security of [company name] assets.

Remember also that you have a shared responsibility for helping keep your co-worker's workspace areas safe and secure also. If you see something that is out-of-place and poses a possible security issue, then notify appropriate personnel immediately.

Computer Workstation Security Requirements

Your computer is one of the most important items to secure, thus the following requirements are to be adhered to at all times by all users:

Computers are to be locked from a logical access control perspective when not in use. This requires initiating a screensaver on the actual computer, or completely shutting the computer down. It is the policy of [company name] to lock access to your computer when left unattended for any period of time. Even going to the restroom, taking a brief water break, or conversing with an employee in close proximity still requires you to invoke the screen saver settings that can only be unlocked with a username and password. Simply put, if your workspace is not occupied by you, then you need to logically and physically secure your computer.

If your computer is not physically taken with you at the end of your work day, then it is to be shut down completely, which means completely powering down the device and not leaving it in "sleep" or "hibernate" mode.

Physical Security Requirements

Computers, if left overnight, must be cable locked or put in a safe place. All other confidential material and items must be securely locked in a file cabinet, etc. Workstations must be left clear and free of any type of item deemed a target by somebody looking to obtain valuable or sensitive information about you, our business, or our clients. The less you leave at your workstation, the better.

Sensitive Information

Company data, personal data, client data – anything deemed sensitive or confidential (i.e., printouts, documents, folder, CD ROMS, etc.) – is to be safely secured at all times when one's workspace is unattended. Such materials should therefore be secured in filing cabinets and/or any other location deemed safe and secure. Remember, our clients expect and demand that their information is always safe and secure, so think before you leave something unattended at your workspace.

Presentation Materials

Any presentation materials used that showcase/illustrate sensitive information is to be removed/cleared from one's workspace when unattended. Whiteboards are one of the most common examples as individuals often use them for "data flowing" sensitive processes and information. "Erase at all times" is the motto to adopt for white boards.

Storage Devices

Removal hard drives, memory sticks, external USB thumb drives – any type of removal storage device – are to be secured at all times when one's workspace is left unattended. Such devices often contain highly sensitive information and are never to be left unattended. Such devices should therefore be secured in file cabinets and/or any other location deemed safe and secure. Take them with you or store them safely somewhere, but never leave them unattended at a workspace.

Unique Identification Information

Passwords, passphrases, social security numbers, dates of birth, client login information – these are just a few examples of the many types of "Unique Identification Information" that should never be left unattended at one's workspace. Often, this information is found on a Post It Note or some other type of sticky pad, which is a clear violation of this stated policy. If you cannot remember some type of unique identification information, then store the credentials in a secure physical space or on your workstation computer where it is safe and secure.

Physical Access Devices

Traditional keys, key FOBs, electronic access control system (ACS) badges – these are also just a few examples of the many types of "Physical Access Devices" that should never be left unattended at one's workspace. An individual with malicious intent can very easily grab such items and immediately begin trying to access rooms, facilities, or other secure locations. Such devices should therefore be secured in file cabinets and/or any other location deemed safe and secure. Take them with you or store them safely somewhere, but never leave them unattended at a workspace.

Secure Disposal of Information

For any items that must be discarded from one's workspace – from paper-based documents to electronic devices – approved disposal methods are to be used, such as incineration, pulverizing, shredding, degaussing, secure wipe, etc. Just because it leaves your workspace, you cannot assume it has been safely disposed of, thus ensure proper protocols are in place for such initiatives.

Printers and Photocopiers & Other Reproduction Technology

Reproduction Technology – such as printers, photocopiers, scanners, digital cameras, etc.) are only to be used in a manner consistent with guidelines provided by the organization. This means using best practices and sound judgement when using any of these technologies.

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 8 - Technological Controls

ISO 27002 Control Coverage: 8.19 – Installation of Software on Operational Systems

Software Installation *Policy and Procedures*

Overview

The Software Installation policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Software Installation policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Software Installation policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Authorized Software: Only authorized software, approved by the IT department or designated personnel, may be installed on organizational operating systems. Unauthorized software, including freeware, shareware, or personal software, is strictly prohibited.

Installation Procedure: Software installations are to follow an approved installation procedure defined by the IT department. This may include utilizing software deployment tools, following specific installation steps, or seeking approval from designated personnel.

Licensing and Compliance: All software installations are to comply with software licensing agreements and adhere to relevant legal requirements. Only licensed software should be installed, and proof of licensing should be maintained and readily available.

Patching and Updates: Installed software is to be regularly updated with the latest patches and updates provided by the software vendor. IT personnel should oversee the patch management process to ensure timely application of updates.

Vulnerability and Compatibility Assessment: Prior to installation, software is to undergo vulnerability and compatibility assessments to identify potential security vulnerabilities, conflicts with existing software, or any adverse effects on system performance.

Malware Prevention: Software installations is to be scanned for malware using approved antivirus software before and after installation to prevent the introduction of malicious code or unauthorized modifications.

Privilege and Access Control: Only authorized individuals with appropriate privileges are to perform software installations. User access rights should be defined based on job roles and responsibilities, granting necessary permissions without excessive privileges.

Logging and Auditing: Records of software installations, including installation date, software version, installer details, and any associated notes, are to be maintained. Regular auditing should be conducted to ensure compliance with this policy.

Uninstallation and Removal: Software that is no longer needed or has reached its end-of-life is to be promptly uninstalled from operating systems to minimize security risks and reduce potential vulnerabilities.

Insert Company Logo

ISO/EIC 27002: Third Edition, 2022-03: Information security, cybersecurity, and privacy protection — Information security controls

Control Theme: Section 8 - Technological Controls

ISO 27002 Control Coverage: 8.20 – Networks Security

Network Security *Policy and Procedures*

Overview

The Network Security policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Network Security policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Network Security policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Management of Network Equipment and Devices

Network Administrator

- Designing, implementing, and maintaining the organization's network infrastructure.
- Configuring and managing network devices such as routers, switches, firewalls, and wireless access points.
- Monitoring network performance, availability, and security.

- Troubleshooting network issues and coordinating with vendors for technical support.
- Implementing network changes and upgrades following change management processes.
- Performing regular backups of network device configurations and ensuring their integrity.
- Managing network access controls and user authentication mechanisms.
- Keeping up-to-date documentation of network configurations, diagrams, and inventory.

System Administrator

- Ensuring the proper installation, configuration, and maintenance of network devices.
- Applying firmware updates, patches, and security fixes to network devices.
- Monitoring network traffic and system logs for security incidents and performance issues.
- Collaborating with network administrators to troubleshoot network connectivity and performance problems.
- Assisting in the design and implementation of network security measures, such as firewalls and intrusion prevention systems.
- Participating in incident response activities and performing forensic analysis when necessary.
- Keeping inventory of network devices, including serial numbers, warranties, and support contracts.

Security Administrator

- Implementing and managing network security policies, procedures, and controls.
- Conducting regular security assessments and vulnerability scans on network devices.
- Managing user access privileges and permissions to network devices.
- Reviewing and updating firewall rules, access control lists (ACLs), and security configurations.
- Monitoring and analyzing network logs for security events and responding to incidents.
- Providing security awareness training to employees and promoting a security-conscious culture.
- Collaborating with the network and system administrators to ensure security best practices are followed.

IT Manager

- Overseeing the management of networking equipment and devices.
- Establishing network management procedures and ensuring compliance with policies and industry regulations.
- Allocating resources for network infrastructure upgrades, maintenance, and expansion.
- Evaluating and selecting network equipment vendors and managing vendor relationships.
- Collaborating with other departments to align network infrastructure with business needs.
- Reviewing and approving network changes, project plans, and budget proposals.
- Monitoring network performance metrics and reporting to senior management.
- Ensuring disaster recovery and business continuity plans for network infrastructure are in place.

Help Desk/Support Team

- Providing first-line support for network-related issues reported by end-users.
- Troubleshooting network connectivity problems and assisting with device configuration.
- Escalating complex network issues to the network and system administrators.
- Assisting in the set-up and configuration of network devices for new employees.
- Conducting basic network troubleshooting for remote users and branch offices.
- Documenting and tracking network-related support requests and resolutions.
- Assisting with user education and training on network device usage and security best practices.

Network Hardening

Secure Configuration Baseline

- Device Hardening Guides: Network devices should be configured according to industry-recognized hardening guides and best practices provided by the device manufacturers or reputable security organizations.

- Secure Protocols: Only secure protocols should be used for device management and communication, such as SSH (Secure Shell) for remote access and HTTPS for web-based management interfaces.
- Default Settings: Default settings, including default usernames, passwords, and IP addresses, should be changed to unique values during the initial device setup to prevent unauthorized access and minimize the risk of exploitation.
- Service Disabling: Unnecessary services and protocols should be disabled or removed from network devices to minimize the attack surface and reduce the risk of potential vulnerabilities.

Access Control and Authentication

- Strong Passwords: Strong passwords should be enforced for device access, including usernames, console access, and remote management interfaces. Password complexity requirements should be defined, and password reuse should be prohibited.
- Multi-Factor Authentication (MFA): Whenever possible, multi-factor authentication (MFA) should be implemented for device access to provide an additional layer of security beyond passwords.
- Access Control Lists (ACLs): Access control lists should be implemented to restrict network device management access to authorized administrators or management subnets.

Firmware and Patch Management

- Vendor Support: Network devices should be covered by active vendor support contracts to ensure access to firmware updates, security patches, and bug fixes.
- Patch Management: Network device firmware should be regularly updated with the latest vendor-released patches and security updates. A patch management process should be established to track, test, and deploy patches in a timely manner.

Network Diagrams

Standardized Network Diagram Format

- Consistency: Network diagrams should follow a standardized format across the organization, ensuring consistency in symbols, colors, labels, and overall layout.
- Legibility: Diagrams should be clear and legible, using appropriate font sizes, line weights, and colors for improved readability.
- Documentation: Each network diagram should include a title, date of creation, version number, and a description of the network segment or area it represents.