SITE CYBERSECURITY PLAN

Test
9/18/2025
Test
brene
SELF ASSESSMENT

Disclaimer

The analysis, data, and reports in CSET® are provided “as is” for informational purposes only. The Cybersecurity & Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

CISA does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by CISA.

The display of the CISA official seal or other CISA visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of CISA. The CISA seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by CISA or the United States Government. Use of the CISA seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against CISA policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office.

Signature

My signature indicates that I have reviewed and approve this Site Cyber Security Plan and the corresponding appendices. To the best of my knowledge, they accurately describe the security profile of the Untitled Assessment 21 security policies and procedures including the operational, management, and technical controls under which they will be operated.

(Example only. Copy and replace the text in this signature block for each applicable position.)

Sample Corporate Officer, CEO John Doe	***Date***

Introduction

Template instructions and directives are given in italicized 10 point font and should be replaced appropriately.

This security plan template is intended to be used as a tool for the development of a security plan. This template will assist you in identifying the controls in place and those needing further implementation based upon the answers provided in the accompanying assessment. The basic process for this plan development would be to first determine risk, second select the countermeasures necessary to mitigate the risk to an acceptable level, and finally follow through to ensure that the countermeasures are implemented to the expected level.

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned, for meeting those requirements. The site cybersecurity plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

The System Owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners, the System Administrator, and the System Security Manager

This template may also include:

- *Recommended templates for policies or procedures that have been identified as needed but not currently available based on the assessment answers.*
- *The basic network diagram*
- *An Inventory List of the components included in the diagram that will be associated with specific controls.*
- *The List of recommended security controls along with a status as can be determined from the assessment questions.*
- *A recommended implementation priorities list. This priority is based on incident occurrences on the Industrial Control System Cyber Emergency Response Team (ICS-CERT) watch floor and cybersecurity expert opinion. These recommendations do not take into account any cost benefit analysis with respect to implementing a control.*
- *Basic security assurance level determinations carried over from the assessment. In developing a security plan it is recommended that a deeper risk analysis is conducted to ensure that the selection of controls is not overly conservative (incurring undo costs) or optimistic (leaving excessive risk exposure).*

1. System Identification

Provide a brief (1-2 paragraphs) description of the main system assests and the necessary protection levels for confidentiality, integrity, and availability. See section 3.1 for a more detailed description of confidentiality, integrity, and availability.

1.1. 1.1. System Environment

Provide a brief (1-3 paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- *The system is connected to the Internet;*
- *It is located in a harsh or overseas environment;*
- *Software is rapidly implemented;*
- *The software resides on an open network used by the general public or with overseas access;*
- *The application is processed at a facility outside of the organization's control; or*
- *The general support mainframe has dial-up lines.*

Describe the primary computing platform(s) used (e.g., mainframe, desk top, LAN or Wide Area Network (WAN). Include a general description of the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

2. Roles and Responsibilities

This section defines the roles and responsibilities for cybersecurity within the company. Use this section to define the roles and responsibilities with respect to this plan for your company.

2.1. Executive Management

Often this role is comprised of the Board of Directors and CEO. Executive management is ultimately responsible for the security of the organization but will most likely delegate tasks and actual implementation.

2.2. Chief Security Officer or Chief Information Security Officer (CISO)

CSO or CISO is the senior level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information related compliance.

Typically, the CISO's influence reaches the whole organization. Responsibilities include:

- Information security and information assurance
- Information regulatory compliance (e.g., US PCI DSS, FISMA, GLBA, HIPAA; UK Data Protection Act 1998; Canada PIPEDA)
- Information risk management
- Supply chain risk management
- Cybersecurity
- Information technology controls for financial and other systems
- Information privacy
- Computer Emergency Response Team / Computer Security Incident Response Team
- Identity and access management
- Security Architecture (e.g. Sherwood Applied Business Security Architecture)
- IT investigations, digital forensics, eDiscovery
- Disaster recovery and business continuity management
- Information Security Operations Center (ISOC)

2.3. Security Steering Committee

The security steering committee is composed of a representative of all the key stakeholders in IT security. These stake holders are often representatives of the executive council, CISO or CSO, IT management, physical security personnel, help desk, and key application and digitial asset owners. This committee meets regularly often quarterly to review policies and procedures, security controls implementation progress, and determine future direction for security within a company.

The security steering committee is responsible for making decisions on tactical and strategic security issues within the enterprise as a whole and should not be tied to one or more business units. The group should be made up of people from all over the organization so they can view risks and the effects of security decisions on individual departments and the organization as a whole. The CEO should head this committee, and the CFO, CIO, department managers, and chief internal auditor should all be on it. This committee should meet at least quarterly and have a well defined agenda. Some of the group's responsibilities are listed next:

- Define the acceptable risk level for the organization.
- Develop security objectives and strategies.
- Determine priorities of security initiatives based on business needs.
- Review risk assessment and auditing reports.
- Monitor the business impact of security risks.
- Review major security breaches and incidents.
- Approve any major change to the security policy and program.

They should also have a clearly defined vision statement in place that is set up to work with and support the organizational intent of the business. The statement shouldbe structured in a manner that provides support for the goals of confidentiality, integrity, and availability as they pertain to the business objectives of the organization. This in turn should be followed, or supported, by a mission statement that provides support and definition to the processes that will apply to the organization and allow it to reach its business goals.

2.4. System Owners

The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

2.5. Data Owners

The data owner (information owner) is usually a member of management who is incharge of a specific business unit, and who is ultimately responsible for the protection and use of a specific subset of information. The data owner has due care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

2.6. Security Administrators

Anyone who has a root account on Unix or Linux systems or an administrator account on Windows or Macintosh systems actually has security administrator rights. (Unfortunately, too many people have these accounts in most environments.) This means they can give and take away permissions and set security configurations. However, just because a person has a root or administrator account does not mean they are fulfilling the security administrator role. A security administrator's tasks are many, and include creating new system user accounts, implementing new security software, testing security patches and components, and issuing new passwords. The security administrator should not actually approve new system user accounts. This is the responsibility of the supervisor. The security administrator must make sure access rights given to users support the policies and data owner directives.

2.7. Supervisors/Managers

The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. The supervisor responsibilities would include ensuring that employees understand their responsibilities with respect to security, distributing initial passwords, making sure the employees' account information is up-to-date, and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access

rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

2.8. Users

The user is any individual who routinely uses the data for work related tasks. The user must have the necessary level of access to the data to perform the duties within their position and is responsible for following operational security procedures to ensure the data’s confidentiality, integrity, and availability to others.

3. Risk Analysis

A good security plan will require that a risk evaluation is performed to determine the level of necessary rigor and cost benefit analysis for the level of controls selected. It is recommended that a general risk analysis be performed. A good risk assessment should include an evaluation of the value of the protected assets and information, an examination of the consequences to the organization in the event of a successful attack, an examination of the threat if possible, and the cost of implementing mitigating controls.

threats × vulnerability × asset value = total risk

total risk – countermeasures = residual risk

Consequence

The examination of the consequences of an attack should include:

- *How many people could sustain injuries requiring a hospital stay?*
- *How many people could be killed?*
- *Estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)*
- *Estimate the potential cost in terms of economic impact to both the site and surrounding communities. (Consider any losses to community structures and any costs associated with displacement.)*
- *Estimate the potential cost of environmental cleanup to the site and surrounding communities. (Consider the cost for cleanup, fines, litigation, long term monitoring, etc.)*

Threat

The threat portion of the equation can be deduced from the recommended implementation priorities list. The priorities are based on incident data collected by the ICS-CERT watch floor and subject matter experts as of the time of publication. Top priorities are controls that mitigate the most actively exploited vulnerabilities with the most significant consequences.

Cost Benefit Analysis

The cost of implementing controls with respect to the additional security provided is the final step in selecting the controls to implement.

3.1 Basic Model

Traditional security models define three areas of consideration Confidentiality, Integrity, and Availability. The security plan should address each of these areas with respect to data and systems.

3.1.1 Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by

limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

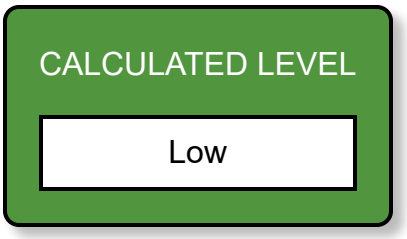
3.1.2 Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID (Atomicity, Consistency, Isolation, Durability) model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

3.1.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

3.2 Security Assurance Level (SAL)



	Confidentiality	Integrity	Availability
Overall Values	Low	Low	Low

4. Security Plan Controls and Status List

This section lists all the controls which constitute the security plan and implementation status. To enable easier reading of the controls list a table key is included at the start of this section. In this section the terms Control and Requirement are used interchangeably to indicate the mitigation effort as defined in the given standard.

Table Key and Field Descriptions:

<table>
<tr><td colspan="2">Requirement Title</td><td>Question/Requirement Category</td></tr>
<tr><td>Control Level</td><td>Implementation Status</td><td>Short Standard Name (Optional, may not be included in the table)</td></tr>
<tr><td colspan="3">Requirement Description</td></tr>
<tr><td colspan="3">Affected Zones (Optional, may not be included in the table)</td></tr>
<tr><td colspan="3">Affected Components (Optional, may not be included in the table)</td></tr>
<tr><td colspan="3">Affected Zones (Optional, may not be included in the table)</td></tr>
</table>

Requirement Title: Is the control title as it is generally defined in the standard document from which this control is derived

Question Category: Shows the question category from the global questions list. Questions from multiple standards have been consolidated together in the tool and assigned a common category.

Control Level: Mapped to one of Low, Moderate, High, or Very High. A value of none indicates that the level was not defined for the given information type in the standard.

Implementation Status: Shows the percentage complete as the number of yes and alternate answers / total related questions for this control. The percentage implemented will not necessarily be reflective of the amount of work required to

implement the control but is merely an indicator of how many of the questions related to the control have been addressed so far.

Short Standard Name (Optional, may not be included in the table): An indicator of which standard this control is derived from.

Control Description: The full control text as defined in the standard from which the control is derived.

Affected Zones (Optional, may not be included in the table): Only applicable to controls derived from a diagram. If you have included a diagram in your original assessment this field will contain a list of zone in which atleast one component was found to require this control.

Affected Components (Optional, may not be included in the table): This field contains a list of the components that are directly applicable to this control.

Related Questions and Answers: A list of the questions and answers from which the implementation status of this control was determined.

6.1		Access Control Management / Access Control Management
Low	100 %	CSC 8
Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.		
Does the organization establish and follow a process for granting access to assets upon new hire, rights grant, or role change?		Yes

6.2		Access Control Management / Access Control Management
Low		CSC 8

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.

Does the organization establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor?	No

6.3		Access Control Management / Access Control Management
Low	100 %	CSC 8
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.		

Does the organization require all externally-exposed or third-party applications to enforce multi-factor authentication?	Yes

6.4		Access Control Management / Access Control Management
Low	100 %	CSC 8
Require MFA for remote network access.		

Does the organization require multi-factor authentication for remote network access?	Yes

6.5		Access Control Management / Access Control Management
Low	100 %	CSC 8
Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.		
Does the organization require multi-factor authentication for all administrative access accounts?		Yes

5.1		Account Management / Account Management
Low	33.33 %	CSC 8
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.		
Does the organization establish and maintain an inventory of all accounts managed?		No
Does the account inventory include the person's name, username, start/stop dates, and department?		No
Does the organization validate that active accounts are authorizes at a defined frequency?		Yes

5.2		Account Management / Account Management
Low		CSC 8
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.		
Does the organization require unique passwords for all assets?		No

5.3		Account Management / Account Management
Low	100 %	CSC 8
Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.		
Does the organization monitor account usage to find dormant accounts and if any are found then disables them and notifies the user or user's manager?		Yes

5.4		Account Management / Account Management
Low		CSC 8
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.		

Does the organization restrict privileged accounts on the information system to organization-defined personnel or roles?	No

8.1		Audit Log Management / Audit Log Management
Low		CSC 8
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.		

Does the organization establish and maintain an audit log management process?	No
Is the audit log management plan reviewed at a defined frequency or when significant changes occur?	No

8.2		Audit Log Management / Audit Log Management
Low	100 %	CSC 8
Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.		

Does the organization collect audit logs?	Yes

8.3		Audit Log Management / Audit Log Management
Low		CSC 8
Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.		

Does the organization ensure that logging destination have adequate storage determined by the management plan?	No

7.1		Continuous Vulnerability Management / Continuous Vulnerability Management
Low		CSC 8
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.		

Is the vulnerability management process reviewed at a defined frequency or with significant changes?	No
Are documented practices followed for threat and vulnerability management activities?	No

7.2		Continuous Vulnerability Management / Continuous Vulnerability Management
Low	50 %	CSC 8
Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.		

Does the organization create a remediation plan to fix security-related issues?	Yes
Is the remediation strategy reviewed at a defined frequency?	No

7.3		Continuous Vulnerability Management / Continuous Vulnerability Management
Low		CSC 8
Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.		

Does the organization deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe?	No

3.1		Data Protection / Data Protection
Low	100 %	CSC 8
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.		

Does the organization establish and maintain a data management process?	Yes
Do data management processes include data sensitivity, data owner, handling of data, data retention limits, and disposal requirements based on the needs of the organization?	Yes
Is data management documentation reviewed and updated at a defined time or when significant changes occur?	Yes

3.2		Data Protection / Data Protection
Low	33.33 %	CSC 8

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.

Does the organization establish and maintain a data inventory?	No
Is sensitive data added to the data inventory?	Yes
Is the data inventory reviewed and updated at a defined time?	No

3.3		Data Protection / Data Protection
Low		CSC 8

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.

Are data access control lists configured based on user's need to know?	No
Does the organization apply permissions to local and remote file systems, databases, and applications?	No

3.4		Data Protection / Data Protection
Low	50 %	CSC 8
Retain data according to the enterprise’s data management process. Data retention must include both minimum and maximum timelines.		

Does the organization have a data retention process?	Yes
Does the data retention process include both minimum and maximum timelines?	No

3.5		Data Protection / Data Protection
Low	100 %	CSC 8
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.		

Does the organization apply a data disposal process?	Yes
Does the data disposal process meet the need based on the sensitivity of the data?	Yes

3.6		Data Protection / Data Protection
Low		CSC 8
Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.		
Does the organization encrypt data on end-user devices when they contain sensitive data?		N/A

11.1		Data Recovery / Data Recovery
Low	66.67 %	CSC 8
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.		
Does the organization establish and maintain a data recovery process?		Yes
Does the recovery process address the scope of data recovery activities, recovery prioritization, and the security of backup data?		Yes
Is the data recovery process reviewed at a defined time or when significant changes occur?		No

11.2	Data Recovery / Data Recovery

Low		CSC 8
Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.		
Does the organization ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information?		No
Does the organization perform automated backups of in-scope assets?		No

11.3		Data Recovery / Data Recovery
Low	100 %	CSC 8
Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.		
Does the organization protect recovery data with equivalent controls to the original data?		Yes

11.4		Data Recovery / Data Recovery
Low	100 %	CSC 8
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.		
Does the organization establish and maintain an isolated instance of recovery data?		Yes

9.1		Email and Web Browser Protections / Email and Web Browser Protections
Low		CSC 8

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.

Does the organization ensure that only fully supported web browsers and email clients are allowed in the organization?	No
Does the organization only use the latest version of browsers and email clients provided via the vendor?	No

9.2		Email and Web Browser Protections / Email and Web Browser Protections
Low		CSC 8

Use DNS filtering services on all enterprise assets to block access to known malicious domains.

Does the organization use DNS filtering on all assets to block malicious domains?	No

17.1		Incident Response Management / Incident Response Management
Low	100 %	CSC 8

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.

Does the organization designate one key person, and at least one backup, who will manage the incident handling process?	Yes
Is the incident handling response process reviewed at a defined frequency or when significant changes occur?	Yes

17.2		Incident Response Management / Incident Response Management
Low	100 %	CSC 8
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.		

Does the organization establish and maintain contact information for parties that need to be informed of security incidents?	Yes

17.3	Incident Response Management / Incident Response Management

Low	100 %	CSC 8
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.		
Does the organization establish and maintain a process for the workforce to report security incidents?		Yes

1.1		Inventory and Control of Enterprise Assets / Inventory and Control of Enterprise Assets
Low	20 %	CSC 8
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.		

Does the organization review and update the information system component inventory per organization-defined frequency?	No
Does the organization maintain an asset inventory of all systems connected to the network and network devices?	No
Does the network asset inventory list contain machine name(s), purpose of each system, responsible asset owner, department associated with each device, IP address and includes desktops, laptops, servers, network equipment, printers, storage area networks, voice over-IP telephones, multi-homed addresses, and virtual addresses?	N/A
Does the network asset inventory also include information on whether the device is portable and/or personal device?	No
Are devices such as mobile phones, tablets, laptops and other portable electronic devices that process data are identified regardless of whether they are attached to the network?	Yes

1.2		Inventory and Control of Enterprise Assets / Inventory and Control of Enterprise Assets
Low		CSC 8
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.		
Does the organization monitor the information system to detect unauthorized network connections?		No

2.1		Inventory and Control of Software Assets / Inventory and Control of Software Assets
Low	33.33 %	CSC 8

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.

Does the organization establish and maintain an inventory of software installed?	Yes
Does the organization's software inventory include the title, publisher, install date, and business purpose?	No
Is the software inventory reviewed and updated?	No

2.2		Inventory and Control of Software Assets / Inventory and Control of Software Assets
Low		CSC 8

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.

Does the organization ensure that only currently supported software is designated as authorized in the software inventory?	No
Does the organization document an exception with mitigating controls and risk acceptance for unsupported but necessary software?	No
Does the organization designate software without exception documentation as unauthorized?	No
Does the organization review their software list to verify software support?	No

2.3		Inventory and Control of Software Assets / Inventory and Control of Software Assets
Low	50 %	CSC 8
Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.		

Does the organization ensure that unauthorized software is either removed from use or receives a documented exception?	Yes
Does the organization review the list of unauthorized software?	N/A

10.1		Malware Defenses / Malware Defenses
Low		CSC 8
Deploy and maintain anti-malware software on all enterprise assets.		

Are antivirus and malware prevention tools documented and implemented?	No

10.2		Malware Defenses / Malware Defenses
Low		CSC 8
Configure automatic updates for anti-malware signature files on all enterprise assets.		
Does the organization configure automatic updates for anti-malware signature files on all assets?		No

10.3		Malware Defenses / Malware Defenses
Low	100 %	CSC 8
Disable autorun and autoplay auto-execute functionality for removable media.		
Does the organization disable auto-run features on systems containing removable media?		Yes

12.1		Network Infrastructure Management / Network Infrastructure Management
Low	100 %	CSC 8

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.

Does the organization ensure network infrastructure is kept up-to-date?	Yes

4.1		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low		CSC 8
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.		

Does the organization have a Configuration Management Plan?	No
Does the organization define the frequency to review and update configuration management procedures?	No
Is the security awareness program mandatory for all employees?	No

4.2		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low	50 %	CSC 8

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.

Does the organization establish and maintain a configuration process for network devices?	Yes
Is the configuration process for network devices reviewed and updated at a defined frequency or after significant changes?	No

4.3		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low	100 %	CSC 8
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.		

Does the information system initiate a session lock after the organization-defined time period of inactivity?	Yes

4.4		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low		CSC 8
Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.		

Does the organization place application firewalls in front of critical servers to verify and validate the traffic going to the server?	Unanswered

4.5		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low	50 %	CSC 8

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.

Does the organization implement and manage a host-based firewall or port-filtering tool on end-user devices?	No
Does the organization apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed?	Yes

4.6		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low	100 %	CSC 8

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.

Does the organization securely manage assets and software using protocols like SSH and HTTPS?	Yes

4.7		Secure Configuration of Enterprise Assets and Software / Secure Configuration of Enterprise Assets and Software
Low	100 %	CSC 8
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.		

Does the organization manage default accounts on assets and software?	Yes

14.1		Security Awareness and Skills Training / Security Awareness and Skills Training
Low		CSC 8

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.

Does the organization have a security awareness program?	No
Are the training materials for the security awareness program updated at least annually?	No

14.2		Security Awareness and Skills Training / Security Awareness and Skills Training
Low	100 %	CSC 8
Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.		

Does the organization include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining?	Yes

14.3		Security Awareness and Skills Training / Security Awareness and Skills Training
Low		CSC 8
Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.		

Does the organization train workforce members on authentication best practices?	No

14.4		Security Awareness and Skills Training / Security Awareness and Skills Training
Low		CSC 8
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.		
Does the organization train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data?		No

14.5		Security Awareness and Skills Training / Security Awareness and Skills Training
Low		CSC 8
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.		
Does the organization train workforce members to be aware of causes for unintentional data exposure?		No

14.6		Security Awareness and Skills Training / Security Awareness and Skills Training
Low	100 %	CSC 8
Train workforce members to be able to recognize a potential incident and be able to report such an incident.		
Does the organization train workforce members to be able to recognize a potential incident and be able to report such an incident?		Yes

14.7		Security Awareness and Skills Training / Security Awareness and Skills Training
Low	50 %	CSC 8
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.		
Does the organization train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools?		No
Does security update training include notifying IT when there are any failures in automated processes and tools?		Yes

14.8		Security Awareness and Skills Training / Security Awareness and Skills Training
Low	100 %	CSC 8

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.

Does the organization train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities?	Yes

15.1		Service Provider Management / Service Provider Management
Low		CSC 8
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.		

Does the organization establish and maintain an inventory of service providers?	No
Does the service provider inventory include all known providers, classifications, and designate a contact for each?	No
Is the service provider inventory reviewed at a defined frequency or with significant changes?	No