PHISH &CHIPS

PHISH & CHIPS
SYSTEM SECURITY PLAN

December 8th, 2025

Mitchell Dees
High Plains Security Consulting

Table of Contents

Table of Contents 1
Executive Summary 2
System Description 3
AC-1 Policy and Procedures (L)(M)(H) 4
AC-6 Least Privilege (M)(H) 7
AC-17(2) Protection of Confidentiality and Integrity Using Encryption (M)(H) 8
AT-2 Literacy Training and Awareness (L)(M)(H) 9
IR-2 Incident Response Training (L)(M)(H) 12
MP-2 Media Access (L)(M)(H) 14
PE-3 Physical Access Control (L)(M)(H) 15
PS-2 Position Risk Designation (L)(M)(H) 18
SA-22 Unsupported System Components (L)(M)(H) 20
SI-3 Malicious Code Protection (L)(M)(H) 22
SI-4(4) Inbound and Outbound Communications Traffic (M)(H) 25
References 27

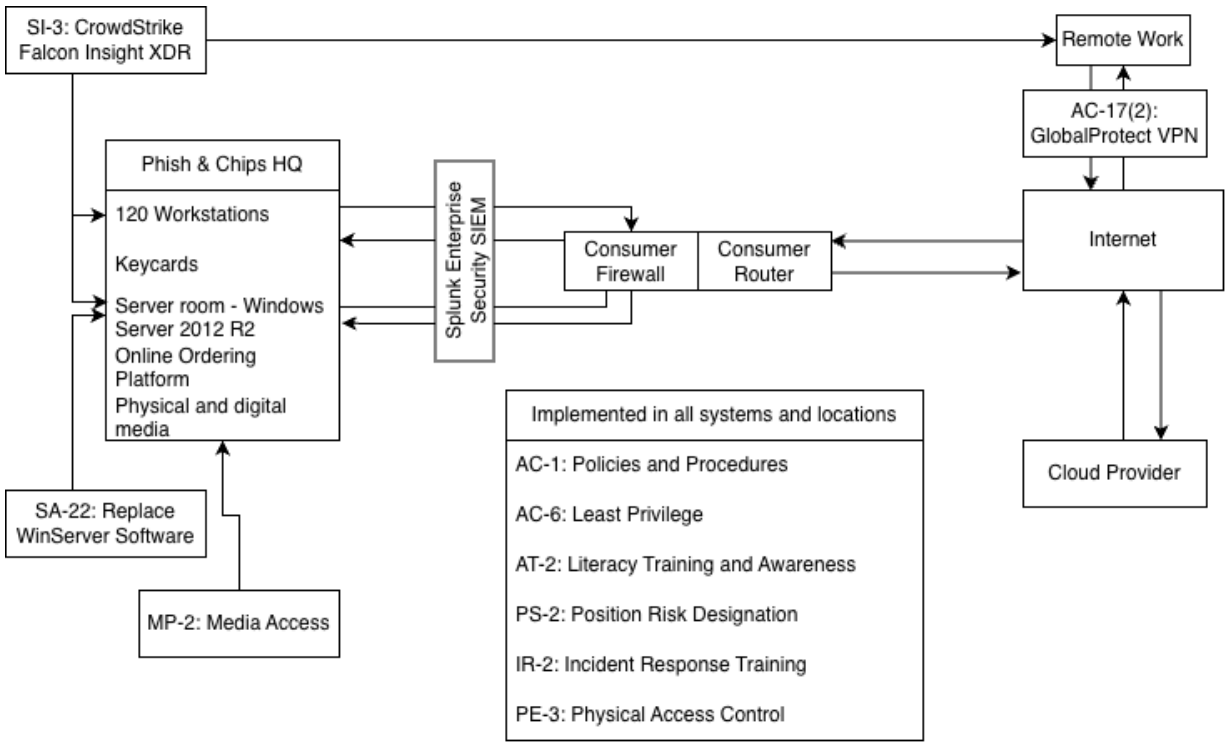
Executive Summary

Phish & Chips is a rapidly expanding business that is onboarding new employees, establishing new locations, and engaging in new product R&D. While this rapid expansion is incredibly fortuitous to Finn Fischer, Chip Frye, and other equity holders, the rate of expansion brings new risks that the management of Phish & Chips must address. This system security plan aims to rectify major security shortcomings of Phish & Chips' IT environment security using controls from the NIST 800-53 framework.

After this executive summary is a brief system description and diagram for the new implementation scheme. The next sections of the document consist of NIST 800-53 security controls to remediate security flaws found after High Plains Security Consulting conducted their security testing and gap analysis. Technical controls include AC-17(2): Protection of Confidentiality and Integrity Using Encryption, SI-3: Malicious Code Protection, and SI-4(4): Inbound and Outbound Communications Traffic. Managerial controls include AC-1: Policies and Procedures, AC-6: Least Privilege, AT-2: Literacy Training and Awareness, PS-2: Position Risk Designation, and IR-2: Incident Response Training. Operational controls include MP-2: Media Access, SA-22: Unsupported System Components, and PE-3: Physical Access Control. Concluding this system security plan is a list of references that aided in the creation of this document.

System Description

The current system does not include an adequate amount of security controls, policies, and procedures to be considered adequately secured. The only security control in place to protect Phish & Chips assets is the consumer-grade routers and firewalls. The main areas of concern stated by the organization are the threat of ransomware and phishing, which will be addressed in the security plan by an EDR solution and staff training. Another issue of concern for Phish & Chips is the lack of personnel screening, system governance, and access controls for their IT environment. The last major issue in Phish & Chips' current security posture is the lack of physical access control and the easy access to physical media in the Denver office.



AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: *organization-defined personnel or roles*]:

1. [Selection (one-or-more): *organization-level; mission/business process-level; system-level*] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: *organization-defined official*] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [Assignment: *organization-defined frequency*] and following [Assignment: *organization-defined events*]; and

2. Procedures [Assignment: *organization-defined frequency*] and following [Assignment: *organization-defined events*].

AC-1 Control Summary Information
Responsible Role: CIO / CISO, Information security manager
Parameter AC-1(a): IT personnel, security team personnel, division managers, store managers
Parameter AC-1(a)(1): Organization-level, business process-level, system-level
Parameter AC-1(b): Information security manager
Parameter AC-1(c)(1)-1: Biennially
Parameter AC-1(c)(1)-2: After security incidents, major threat environment changes, major organization IT architecture changes, new organization divisions added
Parameter AC-1(c)(2)-1: Annually
Parameter AC-1(c)(2)-2: After security incidents, major threat environment changes, major organization IT architecture changes, new organization divisions added, new organization business operations added
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

AC-1 What is the solution and how is it implemented?
Part a: The Phish & Chips CIO/CISO and information security manager must work together to draft and document access control policies. Access control policies must range from granular, such as specific system-level policies, to business process and organization-level policies. Access control policies must follow federal and state laws and regulations applicable to the Phish & Chips IT environment, including Colorado, Washington, Illinois, Wisconsin, California, the District of Columbia, and any other states Phish & Chips will do business in. Access control policy enforcement will be the responsibility of the CIO/CISO and security team director of Phish & Chips. Automated tools should be used to ensure compliance with access control policies across the organization. Implementation of security controls to ensure access control policy compliance will be the responsibility of the security team director. Access control policy compliance will also be reviewed in every Phish & Chips location once a month.
Part b: The Phish & Chips information security manager will be responsible for the continued development and documentation of access control policies and procedures. The document containing all access control policies must be disseminated by the information security manager of Phish & Chips to all IT personnel, security team personnel, division managers, and store managers.
Part c: Access control policies will be reviewed by the Phish & Chips CIO/CISO and information security manager once every two years. Automatic access control policy review will be mandatory if a security incident occurs, major threat environment changes occur, major Phish & Chips IT architecture changes occur, or new Phish & Chips divisions are added. Access control procedures must be reviewed by the Phish & Chips CIO/CISO and information security manager annually. Automatic access control procedure reviews will be mandatory if a

security incident occurs, major threat environment changes occur, major Phish & Chips IT architecture changes occur, new Phish & Chips divisions are added, or new Phish & Chips business operations are added. Policies should be broadly written in a way that survives the test of time longer than granular procedure steps. Access control policies and procedures should “contribute to security and privacy assurance” (CSF Tools, 2024) in the Phish & Chips IT environment.

AC-6 Least Privilege (M)(H)

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AC-6 Control Summary Information
Responsible Role: IT security team, division managers
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

AC-6 What is the solution and how is it implemented?
Both internal personnel and external vendor accounts must be given system access privileges only needed to complete Phish & Chips responsibilities. Least privilege also applies to "system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions" (CSF Tools, 2024). Internal personnel account permissions must be reviewed and approved biannually by Phish & Chips division managers and the security team. Division managers must report account approvals, privileges to be removed, and privileges to be added to the security team for implementation. External accounts, such as vendor accounts, must be audited by the security team once every three months to ensure that vendor access maintains the principle of least privilege. The security team must maintain current documentation on all accounts and disseminate documentation about every account in a division to the division director. Accounts that are not approved within the half-year deadline will be disabled by the security team until the responsible division manager updates the security team with a current audit of said accounts. This process will reduce the risk of privilege creep for Phish & Chips personnel accounts, which also reduces the potential impact of an insider threat or a compromised account due to phishing. Additionally, the process will ensure that internal and external vendor account privileges are managed and always known.

AC-17(2) Protection of Confidentiality and Integrity Using Encryption (M)(H)

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(2) Control Summary Information
Responsible Role: IT security team
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

AC-17(2) What is the solution and how is it implemented?
All Phish & Chips systems and personnel BYOD systems that are used for remote access sessions must connect to the Phish & Chips network using version 6.3 of the Palo Alto Network's GlobalProtect virtual private network service. Any system attempting to remotely connect to the Phish & Chips HQ network or servers without utilizing GlobalProtect 6.3 will be denied. A member of the security team will be designated to teach every Phish & Chips division how to set up and use GlobalProtect for remote access sessions. Phish & Chips personnel will each be assigned a username and a randomly generated password by the security team for initial login to the GlobalProtect. After the security team configures the Phish & Chips corporate account with Palo Alto Networks, they will incrementally implement GlobalProtect onto all Phish & Chips systems used for remote access sessions. Phish & Chips personnel engaging in BYOD will be expected to install the GlobalProtect app on their devices but may request installation assistance from the security team. GlobalProtect 6.3 is available for Windows, Mac, and Linux, along with certain mobile devices. The benefit of a VPN is that it "simulates the security of a dedicated, protected communication line on a shared network" (Pfleeger et al, 2024, p. 494), which enhances security for any remote access sessions taking place outside of the Phish & Chips network.

AT-2 Literacy Training and Awareness (L)(M)(H)

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

   1. As part of initial training for new users and [Assignment: *organization-defined frequency*] thereafter; and

   2. When required by system changes or following [Assignment: *organization-defined events*];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: *organization-defined awareness techniques*];

c. Update literacy training and awareness content [Assignment: *organization-defined frequency*] and following [Assignment: *organization-defined events*]; and

d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

AT-2 Control Summary Information
Responsible Role: Human Resources director, IT security team
Parameter AT-2(a)(1): Biannually
Parameter AT-2(a)(2): After security incidents caused by phishing, after unsuccessful organization phishing tests, major threat environment changes, reports that vendor contact accounts compromised
Parameter AT-2(b): Training seminars, online phishing identification courses, organization phishing tests, biweekly security reminders (email, flyers, etc.), examples of phishing and signs to look out for posted in the office
Parameter AT-2(c)-1: Annually
Parameter AT-2(c)-2: After security incidents caused by phishing, after unsuccessful organization phishing tests, major threat environment changes, vendor changes, changing online training course vendor
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

AT-2 What is the solution and how is it implemented?
Part a: Basic security and threat awareness training is required to be completed by all Phish & Chips personnel during the onboarding process. Furthermore, all Phish & Chips personnel are required to complete ongoing security and threat awareness education biannually, after security incidents caused by phishing, after unsuccessful organization phishing tests, after major threat environment changes, and after reports that vendor contact accounts were compromised. Regular training may be satisfied after an event, as CSF Tools claims that "subsequent literacy training may be satisfied by one or more short ad hoc sessions" (CSF Tools, 2024). Phish & Chips personnel security and awareness training will utilize the Huntress Managed SAT platform. The Huntress Managed SAT platform provides security and personnel awareness training on important topics to the organization, such as phishing, and allows the security team to create custom learning modules based on unique threats that face Phish & Chips. Security and awareness training will cover phishing, social engineering, secure BYOD practices, the risks of shadow IT, secure social media use, and company security policies. AT-2 security and awareness training policies will drastically lower the risk of phishing and other social engineering attacks which were noted as major organizational concerns.
Part b: While the Huntress Managed SAT platform will be primarily used to provide Phish & Chips personnel security and awareness training, other techniques such as brief security reminders, phishing tests, and informational literature will be used as well. Security reminders will be handled via email from the security team with tips, reminders, and real examples of phishing attempts made on Phish & Chips personnel. Up to three phishing tests must be performed every month to measure the awareness of Phish & Chips personnel along with evaluating the current training platform. Informational literature published by NIST and CISA, such as posters and pamphlets, will be made accessible in every office.
Part c: Security and awareness training will be updated by the security team and human resources director annually to adapt to new threats facing Phish & Chips. The training will also be updated after security incidents caused by phishing, after unsuccessful organization phishing tests, major threat environment changes, vendor changes, and changing the online training

course vendor. Updates to security and awareness training must be approved by the human resources director and security team director.
Part d: The security team will ensure that internal lessons learned are incorporated into the security and awareness training by highlighting weak areas, using real examples, and finding more engaging ways for personnel to learn. Internal lessons learned will also be added to the security and awareness training within a week of any major security incidents. Throughout the time between training updates, the security team will be required to perform research on lessons learned by external organizations that may face similar threats as Phish & Chips.

IR-2 Incident Response Training (L)(M)(H)

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

   1. Within [Assignment: *organization-defined time period*] of assuming an incident response role or responsibility or acquiring system access;

   2. When required by system changes; and

   3. [Assignment: *organization-defined frequency*] thereafter; and

b. Review and update incident response training content [Assignment: *organization-defined frequency*] and following [Assignment: *organization-defined events*].

IR-2 Control Summary Information
Responsible Role: CIO/CISO, human resources division director, legal division director, IT security team director, software development division director, finance division director,
Parameter IR-2(a)(1): Ten days for privileged users, two weeks for incident response team members
Parameter IR-2(a)(3): Annually
Parameter IR-2(b)-1: Annually
Parameter IR-2(b)-2: Post major security incident, major threat environment changes, organization division addition, organization business operations addition
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

IR-2 What is the solution and how is it implemented?
Part a: Any role in the Phish & Chips organizational structure that may be responsible for participation in incident response must undergo training when onboarded. Roles that have privileged access to the Phish & Chips systems and IT environment will be required to

complete incident response training no longer than ten days after onboarding. Roles that may be involved with incident response or are a part of the incident response team will be required to complete incident response training no longer than two weeks after onboarding. Training based on roles in incident response may vary, as some "users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents" (CSF Tools, 2024). Incident response training must also be completed by all personnel who are part of the incident response team whenever any major system changes take place. Training for incident response will be required annually for every member of the incident response team. Incident response training ensures that in the event of a major security incident, the response to the event will be efficient and not inadvertently cause more vulnerabilities for threats to exploit.

Part b:

The incident response training program must be reviewed and updated annually. Other reasons that require the reviewal and updating of the incident response training program include major security incidents occurring, major threat environment changes, organization division additions, and organization business operations additions. The review and update processes should be completed and approved by the CIO/CISO, human resources division director, legal division director, IT security team director, software development division director, and finance division director.

MP-2 Media Access (L)(M)(H)

Restrict access to [Assignment: *organization-defined types of digital and/or non-digital media*] to [Assignment: *organization-defined personnel or roles*].

MP-2 Control Summary Information
Responsible Role: IT security team, division managers
Parameter MP-2-1: Internal only digital media, confidential digital media, restricted digital media, internal only physical media, confidential physical media, restricted physical media
Parameter MP-2-2: Phish & Chips executives, division managers, security team, Phish & Chips personnel
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

MP-2 What is the solution and how is it implemented?
The Phish & Chips security team must restrict access to "digital and non-digital media" (CSF Tools, 2024) based on data classification assessments and organizational roles. Authorized and unauthorized access to non-public media must be logged for ongoing monitoring by the security team. The security team must first assess all media in the Phish & Chips environment and classify it based on sensitivity. Classifications used should be public, internal only, confidential, and restricted. The security team, along with division managers, must work together to determine what classification of media every role in the organization is authorized to access. Read, write, and execute controls must be placed on all digital media for all role groups based on the level of classification. Physical media must be protected in locked filing cabinets, with Phish & Chips division managers carrying the key responsible for access. Both physical and digital media access should be tested by the security team once every quarter. Media access control procedures will reduce the risk of insider threats accessing sensitive data, visitors to the office perusing the 2018 financial statements, and malicious actors obtaining the CrispLock recipe.

PE-3 Physical Access Control (L)(M)(H)

a. Enforce physical access authorizations at [Assignment: *organization-defined entry and exit points to the facility where the system resides*] by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using [Assignment (one or more): *[Assignment: organization-defined systems or devices]* , *guards*];

b. Maintain physical access audit logs for [Assignment: *organization-defined entry or exit points*];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: *organization-defined physical access controls*];

d. Escort visitors and control visitor activity [Assignment: *organization-defined circumstances*];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [Assignment: *organization-defined physical access devices*] every [Assignment: *organization-defined frequency*]; and

g. Change combinations and keys [Assignment: *organization-defined frequency*] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

PE-3 Control Summary Information
Responsible Role: CIO / CISO
Parameter PE-3(a): Main office front entrance, main office emergency exits, main office server room, restaurant locations manager office, entrance to actual office space from public lobby
Parameter PE-3(a)(2): Access keycards, guards
Parameter PE-3(b): Main office emergency exits, main office server room
Parameter PE-3(c): Guards
Parameter PE-3(d): Visiting family members, business meeting with Phish & Chips staff, interviewing or screening with human resources, office maintenance, deliveries, government inspections
Parameter PE-3(f)-1: Access keycards
Parameter PE-3(f)-2: Biannually
Parameter PE-3(g): Annually
Implementation Status (check all that apply):

☐ Implemented

☐ Partially Implemented

☒ Planned

☐ Alternative implementation

☐ Not Applicable

PE-3 What is the solution and how is it implemented?

Part a:

Physical access enforcement must be present at the Denver office front entrance, Denver office emergency exits, Denver office server room, and every restaurant location manager's office. Unless it's a public space like restaurant dining areas and the Denver office lobby, all individuals seeking access to non-public spaces must be authorized before they enter said spaces. Access enforcement to non-public spaces will be done using a combination of a security guard in the Denver office lobby and access key cards for all other non-public spaces. Physical access controls will ensure that restricted areas remain safe from threats such as shoulder surfing, physical snooping, and social engineering attacks carried out by walking straight into restricted areas. In *Security in Computing*, Pfleeger claims that there are three approaches to preventing theft which are “preventing access, preventing portability, or detecting exit” (Pfleeger et al, 2024, p. 768), this physical access control plan covers preventing access and detecting exit.

Part b:

Logs must be maintained for any individual access to enter or leave the Denver office server room and any emergency exits in the Denver office. Access logs for these locations should be checked every other week to ensure that correct logging is taking place and physical access control policies are enforced.

Part c:

Phish & Chips must implement a security guard to enforce access control in the Denver office public lobby. The security guard must undergo position risk designated screening before beginning work to ensure the guard itself does not add more risk to physical access to Phish & Chips Denver office.

Part d: Visitors may be escorted by the security guard through the Denver main office for the purpose of visiting family members, business meetings with Phish & Chips staff, interviewing or screening with human resources, office maintenance, deliveries, and government inspections. Unless deemed an emergency or specifically approved by a division manager or senior executive, all other circumstances for access to restricted spaces will be denied.
Part e: Keycards kept by Phish & Chips personnel will be expected to be reasonably secured when not performing responsibilities in the Denver office. If a keycard is lost, Phish & Chips personnel are required to report the keycard loss to the security team within 24 hours. Temporary access keycards must be kept in a locked drawer in the security guard's desk and be issued by the security guard himself for no longer than 48 hours.
Part f: Access keycards must be inventoried for all Phish & Chips personnel biannually by all division managers and reported to the security team and CIO/CISO. Any missing keycards must be disabled, and new keycards must be issued to the personnel that lost said keycards.
Part g: The Phish & Chips security team must change keycard RFID frequency for all personnel annually. Keycard RFID frequency must also change if a keycard is reported as lost or compromised by a gadget like Flipper Zero or when individuals are terminated.

PS-2 Position Risk Designation (L)(M)(H)

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [Assignment: *organization-defined frequency*].

PS-2 Control Summary Information
Responsible Role: Human resources director, security team director
Parameter PS-2(c): Annually
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

PS-2 What is the solution and how is it implemented?
Part a: The human resources director and the security team director will work together to designate the risk level of different roles in the Phish & Chips organization. Designations are defined as low, moderate, and high. Risk designations documentation will be accessible to the human resources team, security team, and executive management. Any new roles or positions added within the Phish & Chips organizational structure will require a risk designation and screening updates. Position risk designation will reduce the risk of the impact of insider threats by thoroughly screening individuals entering higher-risk positions. CSF Tools claims that “Proper position designation is the foundation of an effective and consistent suitability and personnel security program” (CSF Tools, 2024).
Part b: Positions that are designated as low risk, such as servers, cooks, and bussers at physical restaurant locations, will be required to undergo interviews and basic background checks. Moderate-risk positions, such as lower-level accountants, secretaries, and junior software

developers, will be required to undergo the same screening techniques as low-risk individuals with the addition of social media checks and in-depth reference checks. High-risk positions, such as restaurant managers, division managers, security personnel, and executive management, will be required to undergo the screening techniques of both low and moderate-risk positions as well as psychological screening by the human resources director. Human resources personnel, hiring managers, and restaurant managers will be required to complete training on screening techniques up to the highest level of risk designation they personally hire.
Part c: The human resources director and security team director at Phish & Chips will be required to review and update position risk designations on an annual basis. Version-specific copies of the position risk designation documentation should be maintained if an update needs to be rolled back to a baseline that better suits Phish & Chips business operations.

SA-22 Unsupported System Components (L)(M)(H)

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one-or-more): in-house support; [Assignment: *organization-defined support from external providers*]].

SA-22 Control Summary Information
Responsible Role: IT team
Parameter SA-22(b): in-house support
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

SA-22 What is the solution and how is it implemented?
Part a: System components that have reached their end of life and are currently unsupported by the vendor that supplied them must be replaced as soon as possible. CSF Tools defines supported system components as receiving "software patches, firmware updates, replacement parts, and maintenance contracts" (CSF Tools, 2024). All system components used within the Phish & Chips environment must be documented along with their current lifecycle status. Vendors for all system components must be monitored by the security team for any end-of-support announcements. If end of support for any system components is announced, the system component's status must be updated in the documentation. Unsupported system components must be replaced or use alternative sources for continued support before the end-of-support date set by the vendors. Phish & Chips must replace internal server software with Windows Server 2025. The current server operating system is Windows Server 2012 R2, which reached its end of support in October 2023. Other critical systems and networks must be evaluated by the security team to ensure that outdated components are either replaced or are covered by layered security

controls. SA-22 processes will reduce the risk of new vulnerabilities being found and unpatched on systems in the Phish & Chips environment.
Part b: Alternative support through in-house methods may be used if system component replacement is deemed too costly or disruptive to Phish & Chips. In-house support must gain approval from the software development division director and security team director prior to any support work beginning. If approved, the software development team and security team must work together to patch any vulnerabilities found in the software or implement layered controls to mitigate vulnerabilities.

SI-3 Malicious Code Protection (L)(M)(H)

a. Implement [Assignment (one or more): *signature-based*, *non-signature-based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [Assignment: *organization-defined frequency*] and real-time scans of files from external sources at [Assignment (one or more): *endpoint*, *network entry and exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [Assignment (one or more): *block malicious code*, *quarantine malicious code*, *take [Assignment: organization-defined action]*] and send alert to [Assignment: *organization-defined personnel or roles*] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-3 Control Summary Information
Responsible Role: IT security team director
Parameter SI-3(a): Signature-based, non-signature-based
Parameter SI-3(c)(1)-1: Daily
Parameter SI-3(c)(1)-2: Endpoints
Parameter SI-3(c)(2)-1: Block, quarantine, eradicate
Parameter SI-3(c)(2)-2: Security team
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

SI-3 What is the solution and how is it implemented?
Part a: Phish & Chips security team will implement CrowdStrike Falcon Insight XDR for both signature and non-signature-based malicious code protection. Implementation will occur incrementally by division until every endpoint in the Phish & Chips environment is covered. The XDR will also be required to be implemented on any Phish & Chips personnel BYOD used for remote access sessions. CrowdStrike Falcon Insight XDR will detect any malicious code on Phish & Chip's endpoints using known malware signatures and AI-enhanced heuristic analysis. CrowdStrike's non-signature-based protection also satisfies CSF Tool's definition of non-signature-based techniques that "include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective" (CSF Tools, 2024). Once detected, CrowdStrike Falcon Insight XDR will eradicate detected instances of malicious code on endpoints in the Phish & Chips IT environment. Responsibility for malicious code protection ultimately falls to the security team director; however, members of the security team will also be responsible for monitoring the XDR solution. Accounts to access the XDR will be created for senior members of the security team to allow them to monitor the XDR solution. Key performance indicators such as the number of malicious code security incidents, the number of malicious code insertion attempts blocked, and the uptime of all systems in the Phish & Chips environment will be used to review XDR efficacy. The CrowdStrike Falcon Insight XDR will reduce the risk of malware existence in the Phish & Chips IT environment and will mitigate the organizational ransomware concern.
Part b: The Phish & Chips security team will implement updates and patches to CrowdStrike Falcon Insight XDR to all endpoints within a week of release. Implementation will be done incrementally to ensure the continuity of business operations while updating.
Part c: The CrowdStrike Falcon Insight XDR will scan Phish & Chips endpoints daily to ensure that every endpoint is clean. XDR scans will also occur on any file that originates from an external source as they are downloaded and before users can engage in any action with the file. The security team will be required to set up rules determining if malicious code needs to be blocked from transmission, quarantined, or eradicated by the CrowdStrike Falcon Insight

XDR. Any action taken by the XDR must be reported to the security team immediately for further investigation.
Part d: The security team will be required to review all security alerts created by the CrowdStrike Falcon Insight XDR to ensure that actions taken are based on true positives. Frequent false negatives detected by the XDR solution can impact the availability of key Phish & Chips endpoints, which can lead to the major disruption of business operations. If frequent false negatives occur, the security team must take steps to identify the cause and implement new exception rules to the XDR to address the false negatives.

SI-4(4) Inbound and Outbound Communications Traffic (M)(H)

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [Assignment: *organization-defined frequency*] for [Assignment: *organization-defined unusual or unauthorized activities or conditions*].

SI-4(4) Control Summary Information
Responsible Role: IT security team
Parameter SI-4(4)(b)-1: Continuously
Parameter SI-4(4)(b)-2: Unauthorized remote access attempts, sending large packets of data from unknown sources, large packets of data sent from many unknown sources at the same time, large unreported data exfiltration from the Phish & Chips network, inbound traffic not utilizing the Phish & Chips GlobalProtect VPN
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☒ Planned ☐ Alternative implementation ☐ Not Applicable

SI-4(4) What is the solution and how is it implemented?
Part a: Criteria for unusual or unauthorized activities monitored on inbound or outbound communications will be developed by the security team. The security team will be expected to update the criteria for monitoring monthly based on a review of the previous month's unusual activity along with external research. The security team director will be responsible for approving the updated criteria every month along with maintaining documentation on said criteria for monitoring.

Part b:

Phish & Chips will implement the Splunk Enterprise Security application version 10.0.2 across every system and network in their IT environment to monitor all communications traffic. According to Pfleeger, “SIEM tools help organizations recognize and act on security threats and vulnerabilities before they have a chance to disrupt business operations” (Pfleeger, 2024, p. 541). The Splunk Enterprise Security SIEM solution should harden the Phish & Chips network to detect unusual activity so that the security team can stop it before malicious actors can cause damage. Splunk Enterprise Security version 10.0.2 should not interrupt or slow down any existing processes in the Phish & Chips IT environment. The Splunk Enterprise Security SIEM will be monitored continuously by the security team to detect any suspicious activity in the Phish & Chips IT environment. Individual access accounts will be created for each security team member along with the CIO. Criteria determined by the security team will be implemented in the Splunk Enterprise Security SIEM’s security alert rules. Initial criteria include unauthorized remote access attempts, sending large packets of data from unknown sources, large packets of data sent from many unknown sources at the same time, large unreported data exfiltration from the Phish & Chips network, and inbound traffic not utilizing the Phish & Chips GlobalProtect VPN. The incorporation of Splunk Enterprise Security will reduce the risk of DoS/DDoS attacks, unauthorized data theft, unauthorized remote access, and Phish & Chips personnel not adhering to GlobalProtect VPN requirements.

References

CSF Tools. (2024, December 6). *AC-1: Policy and Procedures*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-1/

CSF Tools. (2024, December 6). *AC-6: Least Privilege*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-6/

CSF Tools. (2024, December 6). *AC-17(2): Protection of Confidentiality and Integrity Using Encryption*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-17/ac-17-2/

CSF Tools. (2024, December 6). *AT-2: Literacy Training and Awareness*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/at/at-2/

CSF Tools. (2024, December 6). *AU-6: Audit Records Review*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/au/au-6/

CSF Tools. (2024, December 6). *MP-2: Media Access*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/mp/mp-2/

CSF Tools. (2024, December 6). *PE-3: Physical Access Control*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/pe/pe-3/

CSF Tools. (2024, December 6). *PS-2: Position Risk Designation*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ps/ps-2/

CSF Tools. (2024, December 6). *SA-22: Unsupported System Components*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/sa/sa-22/

CSF Tools. (2024, December 6). *SI-3: Malicious Code Protection*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/si/si-3/

CSF Tools. (2024, December 6). *SI-4(4): Inbound and Outbound Communications Traffic*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/si/si-4/si-4-4/

Pfleeger, C. P., Pfleeger, S. L., & Coles-Kemp, L. (2024). *Security in Computing* (Sixth). Pearson.