IT Security Plan November 2018

Technology Security Plan

Goal: 2018-2022 Goal #1

Reduce System Vulnerabilities

Goal Status: 2. In Progress
Goal Year Implemented: 2017 - 2018
Start Date: 07/01/2017
Goal Priority: High
Key Performance Indicator(s): Assessment reports.

Activities

2. In Progress - Activity #1.1 - Perform authenticated vulnerability scanning: Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. (Active)

Target Completion Date: May 2019
Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.2 - Run Automated Vulnerability Scanning Tools: Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems. (Active)

Target Completion Date: May 2019
Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.3 - Compare Back-to-back Vulnerability Scans: Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. (Active)

Target Completion Date: Ongoing
Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.4 - Protect Dedicated Assessment Accounts: Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. (Active)

Target Completion Date: November 15, 2018
Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.5 - Apply Host-based Firewalls or Port Filtering: 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. Windows 10 Only (Active)

Target Completion Date: TBD (tied to Windows 10 roll-out)
Person Responsible: Manager, Technology

Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.6 - Block connections to known malicious IP addresses (Active)

1. Accomplished - Activity #1.7 - Firewall Training (Active)

Target Completion Date: Spring 2018
Person Responsible: Manager, Technology and Network Specialist
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.8 - Create an Inventory of Network Boundaries. (Active)

Target Completion Date: December 2018
Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.9 - Establish a Process to Accept and Address Reports of Software Vulnerabilities: Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group. (Currently Microsoft only) (Active)

Target Completion Date: February 2019
Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.10 - Anti-Virus/Endpoint Protection (Active)

2. In Progress - Activity #1.11 - Configure Anti-Malware Scanning of Removable Devices: Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. (Active)

Target Completion Date: January 2019
Person Responsible: Network Specialist
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.12 - Utilize an Active Discovery Tool: Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. (Active)

Target Completion Date: February 2019
Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.13 - Default SNMP communities (Active)

Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.14 - Unique passwords on Firewalls, Switches and Routers (Active)

Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.15 - Splunk (Active)

Target Completion Date: May 2019
Person Responsible: Director, Technical Services (assigned to consultant)
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.16 - Windows 10: Don't Run as Admin (Active)

Target Completion Date: TBD (tied to Windows 10 roll-out)
Person Responsible: Director, Technical Services
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #1.17 - Maintain Standard Security Configurations for Network Devices: Maintain standard, documented security configuration standards for all authorized network devices. (Active)

Target Completion Date: Ongoing
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #1.18 - Install the Latest Stable Version of Any Security-related Updates on All Network Devices: Install the latest stable version of any security-related updates on all network devices. (Active)

Target Completion Date: Ongoing
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

1. Accomplished - Activity #1.19 - System Center Configuration Manager (SCCM) (Active)

Person Responsible: Director, Technical Services & Manager, Technology
Activity Year Implemented: 2016 - 2017

2. In Progress - Activity #1.20 - Maintain Inventory of Authorized Software: Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system. (Active)

Target Completion Date: Ongoing
Person Responsible: Director, Computer Services
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.21 - Manage Network Infrastructure Through a Dedicated Network: Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. (Active)

Person Responsible: Director, Technical Services
Activity Year Implemented: 2014 - 2015

1. Accomplished - Activity #1.22 - Do not allow insecure WiFi access points be connected to the network (Active)

Person Responsible: Network Specialists
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.23 - Utilize Software Inventory Tools: Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems. (Active)

Target Completion Date: Ongoing
Person Responsible: Director, Technical Services (assigned to consultant)
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.24 - Integrate Software and Hardware Asset Inventories: The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location. (Active)

Target Completion Date: January 2019
Person Responsible: Director, Technical Services (assigned to consultant)
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.25 - Consistent secure configuration of access points (Active)

Person Responsible: Network Specialists
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.27 - Verify That Acquired Software is Still Supported: Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations. (Active)

Target Completion Date: Ongoing
Person Responsible: Director, Computer Services
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.26 - Do not allow open access points (Active)

Person Responsible: Network Specialists
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.28 - Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data (Active)

Target Completion Date: Fall 2018
Person Responsible: Manager, Technology
Activity Year Implemented: 2016 - 2017

2. In Progress - Activity #1.29 - Maintain an Inventory of Authentication Systems: Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider. (Active)

Target Completion Date: Ongoing
Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.30 - Configure Centralized Point of Authentication: Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems. (Active)

Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #1.31 - Segment network (Active)

Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #1.32 - Switch Configuration (Active)

Target Completion Date: January 2019
Person Responsible: Manager, Technology
Activity Year Implemented: 2017 - 2018

Related Goals

CIS Controls
CIS Control 1 - Inventory and control hardware assets
CIS Control 2 - Inventory and control software assets
CIS Control 3 - Continuous vulnerability management
CIS Control 7 - Protect email and web browsers
CIS Control 8 - Create malware defenses

CIS Control 9 - Limit and control network ports, protocols and services
CIS Control 11 - Secure configuration for network devices
CIS Control 12 - Create effective, multi-layered boundary defenses
CIS Control 13 - Protect sensitive data
CIS Control 15 - Wireless access control
CIS Control 16 - Account monitoring and control
CIS Control 18 - Application software security

Goal: 2018-2022 Goal #2

Improve the Office365 Score to 200 by the end of FY 2018/19

Goal Status: 2. In Progress

Goal Year Implemented: 2017 - 2018
Start Date: 07/01/2017
Goal Priority: High
Key Performance Indicator(s): Office365 score
Score for 10.9.18: 121 of 566

Activities

1. Accomplished - Actvity #2.1 - WSUS Review to verify security patch deployment (Active)

Target Completion Date: Fall 2018
Person Responsible: Network Specialist
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #2.2 - SCCM for secure software deployment (Active)

Person Responsible: Director, Technical Services & Manager, Technology
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #2.3 - Deploy System Configuration Management Tools: Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. (Active)

Target Completion Date: Ongoing using Microsoft Group Policy
Person Responsible: Manager, Technology with Network Specialists
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #2.4 - Spam Protection (Active)

1. Accomplished - Activity #2.5 - Scan all email attachments (Active)

2. In Progress - Activity #2.6 - Use of DNS Filtering Services: Use DNS filtering services to help block access to known malicious domains. (Active)

Target Completion Date: February 2019
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #2.7 - Use multi-factor authentication (Active)

Target Completion Date: Rolling dependent on individual external systems brought online.
Person Responsible: Director, Technical Services & Manager, Technology (with consultants)

Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #2.8 - Activate Audit Logging: Ensure that local logging has been enabled on all systems and networking devices. (Active)

Target Completion Date: December 2018
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #2.9 - Ensure Adequate Storage for Logs: Ensure that all systems that store logs have adequate storage space for the logs generated. (Active)

Target Completion Date: December 2018
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

1. Accomplished - Activity #2.10 - Password Policy (Active)

Person Responsible: Director, Technical Services
Activity Year Implemented: 2014 - 2015

2. In Progress - Activity #2.11 - Maintain Inventory of Administrative Accounts: Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. (Active)

Target Completion Date: November 2018
Person Responsible: Network Specialist
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #2.12 - Regularly Review Logs: On a regular basis, review logs to identify anomalies or abnormal events. (Active)

Target Completion Date: Ongoing
Person Responsible: Network Specialists
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #2.13 - Deploy SIEM or Log Analytic Tool: Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis. (Active)

Target Completion Date: December 2018
Person Responsible: Manager, Technology (with consultant)
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #2.14 - Centralize Anti-malware Logging: Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting. (Active)

Person Responsible: Network Specialist
Activity Year Implemented: 2014 - 2015

2. In Progress - Activity #2.15 - Enable DNS Query Logging: Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains. (Active)

Target Completion Date: January 2019
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

1. Accomplished - Activity #2.16 - Network Time Protocol Server (Active)

Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

Related Goals

CIS Controls
CIS Control 3 - Continuous vulnerability management
CIS Control 4 - Controlled use of administrative privileges
CIS Control 5 - Secure configuration for hardware and software
CIS Control 6 - Maintain, monitor, and analyze audit logs
CIS Control 7 - Protect email and web browsers
CIS Control 8 - Create malware defenses
CIS Control 13 - Protect sensitive data

Goal: 2018-2022 Goal #3

Reduce the number of users/employees who have compromised passwords/email accounts. (Phishing)

Goal Status: 2. In Progress
Goal Year Implemented: 2017 - 2018
Start Date: 07/01/2017
Goal Priority: Medium
Key Performance Indicator(s): Accounts phished by semester. CCC ISC Phishing Assessment

Activities

2. In Progress - Activity #3.1 - Perform a Skills Gap Analysis: Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap. (Active)

Target Completion Date: May 2019
Person Responsible: Director, Technical Services
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #3.2 - Implement a Security Awareness Program: Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner. (Active)

Target Completion Date: May 2019
Person Responsible: IT Security Workgroup
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #3.3 - Train Workforce: Train workforce members on the importance of enabling and utilizing secure authentication. Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls. Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information. Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email. Train employees to be able to identify the most common indicators of an incident and be able to report such an incident. (Active)

Target Completion Date: Ongoing
Person Responsible: IT in collaboration with Human Resources
Activity Year Implemented: 2018 - 2019

Related Goals

CIS Controls
CIS Control 3 - Continuous vulnerability management
CIS Control 7 - Protect email and web browsers
CIS Control 13 - Protect sensitive data
CIS Control 17 - Implement security awareness and training program

Goal: 2018-2022 Goal #4

Establish Incident Response and Management Plans

Goal Status: 2. In Progress
Goal Year Implemented: 2017 - 2018
Start Date: 07/01/2017
Goal Priority: Medium
Key Performance Indicator(s): Incident response plan.

Activities

2. In Progress - Activity #4.1 - Document Incident Response Procedures: Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management. (Active)

Target Completion Date: March 2018
Person Responsible: IT Security Workgroup
Activity Year Implemented: 2017 - 2018

2. In Progress - Activity #4.2 - Maintain Contact Information For Reporting Security Incidents: Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners. (Active)

Target Completion Date: December 2018
Person Responsible: Director, Technical Services
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #4.3 - Conduct Regular External and Internal Penetration Tests: Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. (Active)

Target Completion Date: Ongoing
Person Responsible: Director, Technical Services & Manager, Technology
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #4.4 - Use Vulnerability Scanning and Penetration Testing Tools in Concert: Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts. (Active)

Target Completion Date: Ongoing
Person Responsible: Director, Technical Services & Manager, Technology
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #4.5 - Control and Monitor Accounts Associated with Penetration Testing: Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over. (Active)

Target Completion Date: Ongoing

Person Responsible: Director, Technical Services & Manager, Technology
Activity Year Implemented: 2018 - 2019

1. Accomplished - Activity #4.6 - Use data loss protection software (especially email) (Active)

Person Responsible: Director, Technical Services
Activity Year Implemented: 2017 - 2018

1. Accomplished - Activity #4.7 - Store backups physically secure (Active)

1. Accomplished - Activity #4.8 - Backup Stored Offline (Active)

2. In Progress - Activity #4.9 - Ensure systems backed-up regularly (Active)

Target Completion Date: Ongoing
Person Responsible: Network Specialists
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #4.10 - Test Data on Backup Media: Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working. (Active)

Target Completion Date: Ongoing
Person Responsible: Director, Computer Services
Activity Year Implemented: 2018 - 2019

2. In Progress - Activity #4.11 - Protect Information through Access Control Lists: Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. (Active)

Target Completion Date: March 2019
Person Responsible: Manager, Technology
Activity Year Implemented: 2018 - 2019

Related Goals

CIS Controls
CIS Control 3 - Continuous vulnerability management
CIS Control 10 - Ensure data recovery capability
CIS Control 11 - Secure configuration for network devices
CIS Control 13 - Protect sensitive data
CIS Control 17 - Implement security awareness and training program
CIS Control 19 - Develop and implement Incident response infrastructure
CIS Control 20 - Conduct penetration tests and red team exercises