IS 18 Workstation Administration

Policy Date: December 1, 2017
Applicable to: All Associates
OPR: NOC
INTERNAL POLICY

ALL POLICIES AND PROCEDURES ARE APPROVED BY THE PRESIDENT AND CEO AND APPLY TO ASSOCIATES EMPLOYED WITH MCCALLIE ASSOCIATES, INC. AND ANY SUBSIDIARY COMPANY(IES) UNLESS OTHERWISE STATED. A COMPLETE INDEX MAY BE ACCESSED ELECTRONICALLY ON MCCALLIE'S INTRANET BY CLICKING ON POLICES AND PROCEDURES.

1. PURPOSE

The purpose of this policy is to outline the workstation administration responsibilities and configuration guidance of the McCallie Group Information Systems. These rules are in place to protect the Associate and McCallie. Inappropriate use exposes McCallie to additional risks and legal issues.

2. SCOPE

This policy is intended to cover all workstations owned by the McCallie Group.

3. POLICY

The Network Center is responsible and accountable for the following activities:

- Maintaining a record of whom each workstation is assigned.
- Maintaining an inventory of all hardware, including devices' serial numbers.
- Maintaining a log of the physical location of all hardware.
- Establishing and enforcing security configurations and best practices. (NIST 3.4.2)
- Distributing software to each workstation, including security software and patches. (NIST 3.14.2)
- Maintaining an inventory of all software loaded and ensuring approved software is whitelisted and licensed.
- Ensuring unapproved software is black-listed and removed from workstations. (NIST 3.4.8, 3.4.9)
- Ensuring all hardware is physically marked for ease of identification.
- Clearing and sanitizing any workstations added to or removed from the network or facility. (NIST 3.7.3)
- Executing approved privileged functions, both locally and remotely, including accessing security-relevant information. (NIST 3.1.15)
- Employing systems, processes, and accounts as "least functionality" to allow only essential capabilities on the system to be performed by user-level accounts and permissions. (NIST 3.1.2, 3.4.6, 3.13.3, 3.13.16)
- Monitoring and controlling all information system maintenance tools, techniques, and mechanisms.
- Inspecting these tools for improper or unauthorized modifications or usage.
- Training all personnel responsible for utilizing such items. (NIST 3.7.2)
- Checking media containing diagnostic, test programs, or any media which has any possibility of alteration for malicious code before the media is used in the information system by scanning it with an anti-virus program. (NIST 3.7.4)

System Maintenance

All McCallie Group workstations maintenance will be either completed by the Network Center or under the direct supervision of a Network Center member. Maintenance will be logged and recorded electronically within the Network Center file systems. (NIST 3.7.1, 3.7.6) Information being logged will include:

- Date and time of maintenance.
- Name of individuals or group performing the maintenance.
- Name of escort, if applicable.
- Description of the maintenance performed.
- Description of device being maintained.
- Device components/equipment removed or replaced, including identification numbers, if applicable.

Systems Security

McCallie Group workstations will be securely configured and maintained by the Network Center. The physical security of any workstations signed out to a specific user is the responsibility of that user.

- The Network Center will maintain a log of workstations, including mobile workstations, containing corporate information each time a workstation leaves and returns to the premises. Any workstations not going directly to another McCallie controlled site will have its data removed by the current corporate method.
- All workstations will be configured to automatically lock or log off the network after 10 minutes of inactivity. Users will have to fully authenticate to access the workstation again.
- Workstations will be configured to display a login or lock screen that does not display any sensitive information. (NIST 3.1.10)
- The NOC will employ virus protection software on workstations to prevent transmission of viruses in email attachments, discs, CD-ROMs, and DVDs.
- All workstations will have an easily accessible way to lock the workstation at will. (Example: Keyboard Shortcut of Windows + L to engage the password protected screensaver.)
- All workstations will maintain a log of all system access, including attempted log-ins and administrative tasks which can be uniquely traced back to the user.
- Any assigned identifier pertaining to a user will be immediately disabled or removed upon their termination or reassignment. Identifiers will not be reused for at least two weeks to aid in forensics.

Collaborative Devices

- Collaborative devices, such as web cameras and microphones, will be prevented from being turned on except intentionally by the local user and will display indication of being in use. (NIST 3.13.12)

Workstation Patches

- The NOC will identify, report, and correct information and information system flaws in a timely manner. (NIST 3.14.1)
- All assigned workstations will be patched at a minimum of weekly to install Operating System and software/ application updates.
- All Critical and Security updates for any software on the workstation, including the Operating System, anti-virus, and any installed software/application packages, must be installed within 48 hours of its release. (NIST 3.14.4)
- Discovered vulnerabilities will be remediated in accordance with the assessment of their risk. Higher vulnerabilities will take priority over lower or less likely vulnerabilities. (NIST 3.11.3)

Permitted Actions without Authentication

No actions on workstations can be performed, whether local or nonlocal, without prior multi-factor authentication of user credentials. (NIST 3.5.3, 3.7.5)

4. REFERENCEES

- IS 1, Information Systems Guidelines
- NIST 800-53 Rev4 AC-11 (1) Session Lock | Pattern-Hiding Displays
- NIST 800-53 Rev4 AC-14 Permitted Actions without Identification of Authentication
- NIST 800-53 Rev4 IA-4 Identifier Management
- NIST 800-53 Rev4 SI-2 (2) Flaw Remediation

- NIST 800-53 Rev4 SI-3 (2) Malicious Code Protection | Automatic Updates
- NIST 800-53 Rev4 MA-2 Controlled Maintenance
- NIST 800-53 Rev4 SC-15 Controlled Maintenance
- NIST 800-171 3.1.2, 3.1.10, 3.1.15 Access Control
- NIST 800-171 3.4.2, 3.4.6, 3.4.8, 3.4.9 Configuration Management
- NIST 800-171 3.5.3, 3.5.5, 3.5.6 Identification and Authentication
- NIST 800-171 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6 Maintenance
- NIST 800-171 3.11.3 Risk Assessment
- NIST 800-171 3.13.3, 3.13.12, 3.13.16 System and Communications Protection
- NIST 800-171 3.14.1, 3.14.2, 3.14.4 System and Information Integrity

5. REVISION DETAILS

- New