AC-18 Wireless Access

AC-18(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Nurses and medical technicians need wireless access during the day to carry their remote computers and add patient information onto their online files. Therefore wireless access with be granted during the day, but it will be shut down after closing hours in order to protect user information from potential leaks or over-the-air data theft.

AT-2 Literacy Training and Awareness

AT-2(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES

Provide practical exercises in literacy training that simulate events and incidents.

Run quarterly training of all personnel in training to protect their data, in particular their remote computers and internet connections. This will be done each quarter for both familiarity but also because this office may rotate nurses and technicians over time, so it is important to keep everyone up-to-date on data access and training on detecting and reporting incidents.

AU-12 Event Logging

AU-12(1) AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

CA-6 Authorization

CA-6(1) AUTHORIZATION | JOINT AUTHORIZATION — INTRA-ORGANIZATION

Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

CM-7 Least Functionality

CM-7(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

b. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].

CP-2 Contingency Plan

CP-2(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

Coordinate contingency plan development with organizational elements responsible for related plans.

IA-5 Authentication Management

IA-5(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

For password-based authentication:

a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically-protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

IR-4 Incident Handling

IR-4(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Support the incident handling process using [Assignment: organization-defined automated mechanisms].

MA-4 Nonlocal Maintenance

MA-4(1) NONLOCAL MAINTENANCE | LOGGING AND REVIEW

a. Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; and

b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior

.

MP-7 Media Use

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

PE-2 Physical Access Authorizations

E-2(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE

Authorize physical access to the facility where the system resides based on position or role.

PL-7 System Security and Privacy Plans

a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and

b. Review and update the CONOPS [Assignment: organization-defined frequency].

PS-5 Personnel Transfer

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [ Assignment: organization-defined time period following the formal transfer action];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

RA-3 Risk Assessment

RA-3(1) RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT

a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and

b. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

SA-5 System Documentation

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; a nd

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and

d. Distribute documentation to [Assignment: organization-defined personnel or roles].

SC-12 Cryptography Key Establishment

SC-12(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

Maintain availability of information in the event of the loss of cryptographic keys by users.

SI-4 System Monitoring

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SR-10 System Monitoring

Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].