NYLE

FedRAMP Moderate Templates

Access Control Family Implementation Checklist

Policy and Documentation (AC-1)

- □ Develop and document access control policy at organization, mission/business process, and/or system levels
- □ Create procedures for implementing access control policy and controls
- □ Designate an official to manage access control policy and procedures
- □ Review and update policy at least every 3 years and after significant events
- □ Review and update procedures at least annually and after significant changes
- □ Disseminate policy and procedures to relevant personnel

Account Management (AC-2)

- □ Define and document allowed and prohibited account types
- □ Assign account managers for all systems
- □ Establish prerequisites and criteria for group and role membership
- □ Document authorized users, group/role memberships, and access privileges
- □ Require approvals for account creation requests
- □ Implement processes to create, enable, modify, disable, and remove accounts
- □ Monitor account usage continuously
- □ Notify account managers within 24 hours when accounts are no longer needed
- □ Notify relevant personnel within 8 hours when users are terminated or transferred
- □ Notify relevant personnel within 8 hours when user access needs change
- □ Review accounts for compliance at least annually
- □ Establish process for changing shared/group account authenticators when members are removed
- □ Align account management with personnel termination/transfer processes

Account Management Enhancements

- □ **AC-2(1):** Implement automated system account management tools
- □ **AC-2(2):** Automatically disable temporary and emergency accounts after 30 days from last use
- □ **AC-2(3):** Disable expired, unassociated, policy-violating accounts within 24 hours; inactive accounts within 90 days
- □ **AC-2(4):** Automatically audit all account creation, modification, enabling, disabling, and removal actions
- □ **AC-2(5):** Require users to log out after defined periods of inactivity
- □ **AC-2(7):** Establish privileged accounts using role-based or attribute-based access schemes
- □ **AC-2(7):** Monitor privileged role assignments and changes
- □ **AC-2(7):** Revoke access when privileged assignments are no longer appropriate
- □ **AC-2(9):** Only allow shared/group accounts with documented business justification
- □ **AC-2(12):** Monitor accounts for atypical usage patterns
- □ **AC-2(12):** Report atypical usage to ISSO and similar security roles
- □ **AC-2(13):** Disable high-risk individual accounts within 1 hour of risk discovery

Access Control Enforcement (AC-3, AC-4, AC-5, AC-6)

- □ **AC-3:** Enforce approved authorizations for logical access to information and system resources
- □ **AC-4:** Control information flow within and between systems per organizational policies
- □ **AC-5:** Identify duties requiring separation and define supporting access authorizations
- □ **AC-6:** Implement least privilege principle for all users and processes

Least Privilege Enhancements

- □ **AC-6(1):** Authorize specific individuals/roles for security function access
- □ **AC-6(2):** Require users with security function access to use non-privileged accounts for non-security tasks
- □ **AC-6(5):** Restrict privileged accounts to designated personnel/roles only
- □ **AC-6(7):** Review all user privileges at least annually and adjust as needed
- □ **AC-6(9):** Log execution of all privileged functions

- □ **AC-6(10):** Prevent non-privileged users from executing privileged functions

Session Controls (AC-7, AC-8, AC-11, AC-12)

- □ **AC-7:** Limit invalid logon attempts to maximum 3 consecutive attempts within 15 minutes
- □ **AC-7:** Lock accounts/nodes for minimum 30 minutes or until administrator unlocks after exceeded attempts
- □ **AC-8:** Display system use notification banner before granting access
- □ **AC-8:** Require user acknowledgment of usage conditions before system access
- □ **AC-8:** Configure appropriate notifications for publicly accessible systems
- □ **AC-11:** Initiate device lock after 15 minutes of inactivity
- □ **AC-11:** Require users to initiate device lock when leaving system unattended
- □ **AC-11(1):** Conceal information on locked displays with publicly viewable images
- □ **AC-12:** Automatically terminate user sessions based on defined conditions/events

Remote and Wireless Access (AC-14, AC-17, AC-18)

- □ **AC-14:** Identify and document actions allowed without authentication
- □ **AC-14:** Provide rationale in security plan for unauthenticated actions
- □ **AC-17:** Document usage restrictions and requirements for each remote access type
- □ **AC-17:** Authorize each remote access type before allowing connections
- □ **AC-17(1):** Use automated mechanisms to monitor and control remote access
- □ **AC-17(2):** Implement cryptographic protection for remote access sessions
- □ **AC-17(3):** Route remote access through authorized network access control points
- □ **AC-17(4):** Restrict privileged remote access and document rationale in security plan
- □ **AC-18:** Establish requirements and guidance for each wireless access type
- □ **AC-18:** Authorize wireless access types before allowing connections
- □ **AC-18(1):** Implement authentication and encryption for wireless access
- □ **AC-18(3):** Disable unused wireless networking capabilities before deployment

Mobile Device Management (AC-19)

- □ **AC-19:** Establish configuration and connection requirements for mobile devices
- □ **AC-19:** Define implementation guidance for mobile devices outside controlled areas

- □ **AC-19:** Authorize mobile device connections to organizational systems
- □ **AC-19(5):** Implement full-device or container-based encryption on mobile devices

External System Controls (AC-20, AC-21, AC-22)

- □ **AC-20:** Establish terms/conditions or identify required controls for external systems
- □ **AC-20:** Allow authorized access from external systems per established trust relationships
- □ **AC-20:** Prohibit use of unauthorized external system types
- □ **AC-20(1):** Verify external system controls or maintain connection agreements
- □ **AC-20(2):** Restrict use of organization-controlled portable storage on external systems
- □ **AC-21:** Enable users to verify sharing partner access authorizations match information restrictions
- □ **AC-21:** Implement mechanisms to assist with information sharing decisions
- □ **AC-22:** Designate individuals authorized to make information publicly accessible
- □ **AC-22:** Train authorized individuals on protecting nonpublic information
- □ **AC-22:** Review content before posting to publicly accessible systems
- □ **AC-22:** Review publicly accessible content at least quarterly and remove nonpublic information