Establish lockout procedures or lockout mechanisms to be triggered after a predetermined number of consecutive logon attempts.

CONTROL ID
01412

CONTROL TYPE
Technical Security

CLASSIFICATION
Preventive

SUPPORTING AND SUPPORTED CONTROLS

This Control directly supports the implied Control(s):

- Control access rights to organizational assets., CC ID: 00004

This Control has the following implementation support Control(s):

- Disallow unlocking user accounts absent system administrator approval., CC ID: 01413

SELECTED AUTHORITY DOCUMENTS COMPLIED WITH

- User accounts should be locked after 3 unsuccessful logon attempts. **(§ 3.6.18, Australian Government ICT Security Manual (ACSI 33))**
- PEDs should be set to zeroize after 3 unsuccessful passwords have been entered during the login process. **(§ 2.3.2 (2.3.2.030), The Center for Internet Security Wireless Networking Benchmark, 1)**
- System access should be revoked after a predetermined number of unsuccessful logon attempts. **(¶ 19.3 Bullet 8, Good Practices For Computerized systems In Regulated GXP Environments)**
- The organization must prevent consumer access to secure data, following three failed logon attempts. **(§ 2b, American Express Data Security Standard (DSS))**
- Are repeated access attempts limited by locking out the user ID after no more than six attempts? **(8.1.6 (a), Payment Card Industry (PCI) Data Security Standard, Self-Assessment Questionnaire D and Attestation of Compliance for Merchants, Version 3.1)**
- Are repeated access attempts limited by locking out the user ID after no more than six attempts? **(8.1.6 (a), Payment Card Industry (PCI) Data Security Standard, Self-Assessment Questionnaire D and Attestation of Compliance for Service Providers, Version 3.1)**
- For service providers only: Are non-consumer customer passwords temporarily locked-out after not more than six invalid access attempts? **(8.1.6 (b), Payment Card Industry (PCI) Data Security Standard, Self-Assessment Questionnaire D and Attestation of Compliance for Service Providers, Version 3.1)**
- The organization should lock out account access after a predetermined number of unsuccessful attempts to log onto the web site. **(Pg 70, VISA E-Commerce Merchants Guide to Risk Management Tools and Best Practices for Building a Secure Internet Business)**
- General application security controls must be reviewed when the application's logical access controls are performed, including ensuring accounts are locked out after a predefined number of unsuccessful login attempts. **(§ 4 (Access Controls) ¶ 2, IIA Global Technology Audit Guide (GTAG) 8: Auditing Application Controls)**
- The system should be configured to prevent users from continually trying passwords to gain access to the system by setting the number of invalid attempts permitted before locking the system. **(Pg 12-II-42, Pg 12-IV-4, Protection of Assets Manual, ASIS International)**
- Sign-on mechanisms should be configured so that they limit the number of unsuccessful sign-on attempts which are permitted (e.g., a re-try limit of three). **(CF.06.07.02b, The Standard of Good Practice for Information Security)**
- Mobile devices should be protected by the use of device lock-out and deletion of all information stored on the device following multiple failed authentication attempts (e.g., ranging from 3 incorrect passwords in succession

- The system should lock accounts after a set number of failed logon attempts for a predetermined amount of time. **(Critical Control 16.9, Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, Version 4.0)**
- The system should be able to detect when unsuccessful authentication attempts occur and take action; when a defined number of unsuccessful attempts have been attempted, the system should have the ability to disable the account or terminal for a certain amount of time or disable the account until unl... **(§ 12.1, § G.1, ISO 15408-2 Common Criteria for Information Technology Security Evaluation Part 2, 2008)**
- The number of unsuccessful logon attempts should be limited. **(§ 11.5.1, ISO 27002 Code of practice for information security management, 2005)**
- Limit the number of unsuccessful authentication attempts; or **(CIP-007-6 Table R5 Part 5.7 Requirements ¶ 1 Bullet 1, North American Electric Reliability Corporation Critical Infrastructure Protection Standards Cyber Security - System Security Management CIP-007-6, Version 6)**
- On UNIX computers or Linux computers that transmit scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.16.22, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On UNIX computers or Linux computers that process scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.16.22, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On UNIX computers or Linux computers that store scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.16.22, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On windows systems that transmit scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.17.20, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On windows systems that process scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.17.20, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On windows systems that store scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.17.20, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On mainframes that transmit scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.18.22, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**

G. Communications and Operations Management, 7.0)

- On as400 systems that process scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.19.20, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On as400 systems that store scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.19.20, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On open vms (vax or alpha) systems that transmit scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.20.17, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On open vms (vax or alpha) systems that process scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.20.17, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- On open vms (vax or alpha) systems that store scoped data, does the system lock an account when three to five invalid login attempts are made? **(§ G.20.17, Shared Assessments Standardized Information Gathering Questionnaire - G. Communications and Operations Management, 7.0)**
- For cloud computing services that use a hypervisor to transmit, process, or store scoped data, does the system lock an account when 3 to 5 invalid login attempts are made? **(§ V.1.72.21, Shared Assessments Standardized Information Gathering Questionnaire - V. Cloud, 7.0)**
- The number of user logon attempts should be limited to 3 on classified and unclassified-sensitive systems. The user should not be allowed back on the system until the Information System Security Officer has verified the reason for the lockout. **(§ 2-24.e, Army Regulation 380-19: Information Systems Security, February 27, 1998)**
- Table F-3: For Windows 2000 Professional, the organization must configure the system to enable account lockout after a specific length of time. Table F-4: For Windows XP Professional, the organization must configure the system to enable account lockout after a specific length of time. **(Table F-3, Table F-4, CMS Business Partners Systems Security Manual, Rev. 10)**
- The organization must configure systems to disable access for 15 minutes after 3 failed logon attempts. After 3 consecutive failed logon cycles, the user account must be locked and access must require an administrator to reset the account and restore access. **(CSR 2.9.10, Pub 100-17 Medicare Business Partners Systems Security, Transmittal 7, Appendix A: CMS Core Security Requirements CSR, March 17, 2006)**
- After three unsuccessful attempts to log on, the user is locked out of the system and the IT administrator must reinstate the user's access. **(Pg 46, C-TPAT Supply Chain Security Best Practices Catalog)**

denied. **(§ 8-609.a(2), NISPOM - National Industrial Security Program Operating Manual (DoD 5220.22-M) February 26, 2006, February 28, 2006)**

- The system shall enforce a limit of no more than 5 consecutive invalid access attempts to systems with criminal justice information or access to criminal justice information. **(§ 5.5.3, Criminal Justice Information Services (CJIS) Security Policy, CJISD-ITS-DOC-08140-5.2, Version 5.2)**
- Access controls include password complexity and limits to password attempts and reuse. **(Domain 3: Assessment Factor: Preventative Controls, ACCESS AND DATA MANAGEMENT Baseline 1 ¶ 7, FFIEC Cybersecurity Assessment Tool, Baseline, May 2017)**
- The system should lock out access to the customer's account after a predefined number of unsuccessful personal identification number (PIN) attempts. **(Pg 40, Exam Tier II Obj 2.5, FFIEC IT Examination Handbook - Retail Payment Systems, March 2004)**
- Procedures shall be in place to prevent the unauthorized use of identification codes and/or passwords and to detect and report attempts at unauthorized uses immediately and urgently to the system security unit and the organizational management in order to ensure the security and integrity of the ele... **(§ 11.300(d), 21 CFR Part 11, Electronic Records; Electronic Signatures)**
- The system must be configured to disable an account after 3 unsuccessful login attempts. **(§ 5.6.1, Exhibit 4 AC-7, Exhibit 8 Control 10, IRS Publication 1075: TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES AND ENTITIES; Safeguards for Protecting Federal Tax Returns and Return Information)**
- Does the computer system lock out users after a predetermined number of failed logon attempts? **(IT - General Q 14, Automated Integrated Regulatory Examination System (AIRES) IT Exam Questionnaires, version 073106A)**
- Do the written procedures for internet banking User IDs and passwords include the maximum number of unsuccessful logon attempts before locking out the user? **(IT - Member Online Services Q 12c, Automated Integrated Regulatory Examination System (AIRES) IT Exam Questionnaires, version 073106A)**
- Do written procedures for bill payer User IDs and passwords include the maximum unsuccessful logon attempts before locking out the user, if users log in to the bill payer software separately from the internet banking software? **(IT - Member Online Services Q 32c, Automated Integrated Regulatory Examination System (AIRES) IT Exam Questionnaires, version 073106A)**
- Are account lockout options enabled? **(IT - Networks Q 9, Automated Integrated Regulatory Examination System (AIRES) IT Exam Questionnaires, version 073106A)**
- § 3.2.7: The organization should limit the number of incorrect password attempts users are allowed to protect against exhaustive search attacks. § 4.5 ¶ 1: The organization should limit the number of consecutive incorrect

of time and the accounts remain locked for a defined period of time before allowin... **(AC-7, AC-7.5, Guide for Assessing the Security Controls in Federal Information Systems, NIST SP 800-53A)**

- The AP login screen should be locked after a predefined number of unsuccessful attempts. **(§ 6.3.3.1(Configuring administrator access), Guide to Securing Legacy IEEE 802.11 Wireless Networks, NIST SP 800-48, Revision 1)**
- The smart grid Information System must be configured to limit the number of consecutive unsuccessful login attempts during a named time period. **(SG.AC-8 Requirement, NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, August 2010)**
- Limit unsuccessful logon attempts. **(3.1.8, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, NIST Special Publication 800-171)**
- Limit unsuccessful logon attempts. **(3.1.8, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, NIST Special Publication 800-171, Revision 1)**
- The organization must establish and maintain unsuccessful login attempt policies and procedures to enforce a defined limit of consecutive invalid access attempts by a user in a named period of time. **(App F § AC-7.a, Recommended Security Controls for Federal Information Systems, NIST SP 800-53)**
- The organization should automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded. **(App F § AC-7(1), Recommended Security Controls for Federal Information Systems, NIST SP 800-53)**
- The organization should provide additional protection for mobile devices accessed via login by purging information from the device after a defined number of consecutive, unsuccessful logon attempts. **(App F § AC-7(2), Recommended Security Controls for Federal Information Systems, NIST SP 800-53)**
- The organization must use compensating controls in accordance with the general tailoring guidance when the Industrial Control System cannot support account locking, node locking, or delayed logins or the Industrial Control System cannot conduct account locking, node locking, or delayed logins becaus... **(App I § AC-7, Recommended Security Controls for Federal Information Systems, NIST SP 800-53)**
- The information system enforces a limit of {organizationally documented number} consecutive invalid logon attempts by a user during a {organizationally documented time period}. **(AC-7a., Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Revision 4)**
- The information system purges/wipes information from {organizationally documented mobile devices} based on {organizationally documented purging/wiping requirements/techniques} after {organizationally documented number} consecutive, unsuccessful device logon attempts. **(AC-7(2), Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Revision 4)**

for Federal Information Systems and Organizations, NIST SP 800-53, Moderate Impact Baseline, Revision 4)

- Anyone who stores, licenses, owns, or maintains personal information about a Massachusetts resident and electronically transmits or stores that information must establish and maintain a security system (which must be included in the comprehensive, written information security program) for all comput... **(§ 17.04(1)(e), Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts)**

Stay connected with UCF

Subscribe to UCF news and alerts

Contact

244 Lafayette Circle
Lafayette, CA 94549
PHONE 510.962.5192
FAX 866.924.3791
info@unifiedcompliance.com