Minimum Security Standard for Electronic Information (effective July 2013)

PLEASE NOTE THAT ANY URLS CONTAINED BELOW MIGHT BE OUT OF DATE.

FOR THE UPDATED MSSEI GO TO: https://security.berkeley.edu/minimum-security-standards-electronic-information

This standard has been revised.
Please see Minimum Security Standards for Electronic Information (effective 2014) (https://security.berkeley.edu/node/363) for the latest revision.

*The following **Minimum Security Standard for Electronic Information (MSSEI)** is issued under the authority vested in the UC Business Finance Bulletin IS-3 Electronic Information Security (http://www.ucop.edu/ucophome/policies/bfb/is3.pdf): "All campuses shall establish an Information Security Program (Program) in conformance with the provisions in this bulletin. In order to achieve a secure information technology environment, the campus Program shall comprise a comprehensive set of strategies that include a range of related technical and non-technical measures." (Section III)*

Issue Date: *July 16, 2012*
Effective Date: *July 16, 2013*
Supersedes: Minimum Security Standards for Electronic Information (Issued: November 1, 2009/Effective: January 1, 2010)

Responsible Executive: Associate Vice Chancellor for Information Technology and Chief Information Officer
Responsible Office: Berkeley Privacy Office

Contact: IT Policy Manager, itpolicy@berkeley.edu (mailto:itpolicy@berkeley.edu)

Table of Contents

Scope and Background

Covered Data

This Minimum Security Standard for Electronic Information (MSSEI) defines the minimum set of confidentiality controls for Protection Level 2 data as defined in the Berkeley Data Classification Standard (https://security.berkeley.edu/node/280). Protection Level 2 data includes California State Law notice-triggering information (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29) (Civil Code 1798.29, formerly SB1386/AB1298 data), which is defined as:

First name OR first initial and last name in combination with one or more of the following:

- Social security number,
- Driver's license number,
- California identification number,
- Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account,
- Medical information,

- Health insurance information.

Covered Devices

Each control in this standard applies to one or more of the following devices:

- **Core System devices:** Database servers; application servers; web front-end servers; back-up and storage systems that store, process, or transmit covered data; and any systems that provide authentication, authorization, or configuration management for those systems.
- **Sys Admin devices:** Any device used with privileged access (super user, root, administrator, database administrator, and equivalent) to a core system device (physical, logical, and virtual devices included).
- **Bulk Access devices:** Any device used with credentials that have access to 500 or more covered data records in bulk transactions or any device that stores 500 or more covered data records.
- **Client devices:** Any device accessing covered data not listed above as a covered device or listed below as not covered.

The following devices are not covered under this standard:

- Infrastructure service devices (e.g., DNS servers, NTP servers)
- Network infrastructure devices (e.g., switches/routers)

Background

The MSSEI is derived from industry-accepted best practices for cyber defense, such as the SANS 20 Critical Security Controls (http://www.sans.org/critical-security-controls/).

Device-Control Summary

Application of Controls to Covered Device Types

Control	Core System Devices	Sys Admin Devices	Bulk Access Devices	Client Devices	Guidelines

1: Annual Registration (https://security.berkeley.edu/mssei-2013#registration)

Required

Required

Recommended

1.1 Covered System Registration (https://security.berkeley.edu/node/394)
1.2 Registration Review (https://security.berkeley.edu/node/395)

2: Managed Software Inventory (https://security.berkeley.edu/mssei-2013#software-inventory)

Required

Required

Recommended

Recommended

2.1 Mananged Software Inventory (https://security.berkeley.edu/node/396)

3: Secure Device Configurations (https://security.berkeley.edu/mssei-2013#configurations)

Required

Required

Required

Required

3.1 Secure Device Configuration (https://security.berkeley.edu/node/397)

4: Continuous Vulnerability Assessment and Remediation (https://security.berkeley.edu/mssei-2013#vulnerability-assessment)

Required

Required

Recommended

Recommended

4.1 Vulnerability Assessment and Remediation (https://security.berkeley.edu/node/398)
4.2 Authenticated Scans (https://security.berkeley.edu/node/399)
4.3 Intrusion Detection (https://security.berkeley.edu/node/400)

5: Malware Defenses (https://security.berkeley.edu/mssei-2013#malware)

Required

Required

Required

Required

5.1 Malware Defense (https://security.berkeley.edu/node/401)
5.2 Auto-Run Configuration (https://security.berkeley.edu/node/402)

6: Application Software Security (https://security.berkeley.edu/mssei-2013#application)

Required

6.1 Secure Coding Practice (https://security.berkeley.edu/node/403)
6.2 Application Security Testing (https://security.berkeley.edu/node/354)
6.3 Commercial Software Assessment (https://security.berkeley.edu/node/427)

7: Mobile and Wireless Device Control (https://security.berkeley.edu/mssei-2013#mobile)

Required

Required

Required

Required

7.1 No Core system on Mobilie/Wireless Devices (https://security.berkeley.edu/node/405)
7.2 Data Encryption at Rest (https://security.berkeley.edu/node/379)
7.3 Data Encryption in Transit (https://security.berkeley.edu/node/391)

8: Privacy & Security Training (https://security.berkeley.edu/mssei-2013#training)

Required

Required

Required

Required

8.1 Security and Privacy Training (https://security.berkeley.edu/node/406)

9: Separation of System Resources (https://security.berkeley.edu/mssei-2013#separation)

Required

9.1 Separation of System Resources (https://security.berkeley.edu/node/407)

10: Controlled Use of Administrative Privileges (https://security.berkeley.edu/mssei-2013#admin)

Required

Required

Required

10.1 Use of Admin Accounts on Secure Devices (https://security.berkeley.edu/node/408)
10.2 Admin Account Security (https://security.berkeley.edu/node/409)

11: Boundary Defense (https://security.berkeley.edu/mssei-2013#boundary)

Required

11.1 Managed Hardware Firewall (https://security.berkeley.edu/node/410)
11.2 Protected Subnet (https://security.berkeley.edu/node/411)

12: Audit Logging (https://security.berkeley.edu/mssei-2013#logs)

Required

12.1 Audit Logging (https://security.berkeley.edu/node/412)

13: Controlled Access Based on the Need to Know (https://security.berkeley.edu/mssei-2013#need-to-know)

Required

Required

Required

Required

13.1 Controlled Access Based on Need to Know (https://security.berkeley.edu/node/413)

14: Account Monitoring and Management (https://security.berkeley.edu/mssei-2013#account)

Required

Required

Required

Required

14.1 Account Monitoring and Management (https://security.berkeley.edu/node/414)

15: Data Loss Prevention (https://security.berkeley.edu/mssei-2013#dlp)

Required

Required

Required

Required

15.1 Data Encryption in transit (https://security.berkeley.edu/node/391)
15.2 Data Encryption on Removable Media (https://security.berkeley.edu/node/379)
15.3 Secure Deletion (https://security.berkeley.edu/node/392)
15.4 Data Access Agreement (https://security.berkeley.edu/node/342)

16: Incident Response Capability (https://security.berkeley.edu/mssei-2013#incident-response)

Required

16.1 Incident Response Planning (https://security.berkeley.edu/node/415)
16.2 Incident Response Plan Availability (https://security.berkeley.edu/node/416)
16.3 Incident Response Training (https://security.berkeley.edu/node/417)

17: MSSND Compliance (https://security.berkeley.edu/mssei-2013#mssnd)

Required

Required

Required

Required

MSSND Guidelines (https://security.berkeley.edu/MinStds/netdevices.html#guidelines)

1: Annual Registration

(SANS Critical Control 1: Inventory Of Authorized And Unauthorized Devices (http://www.sans.org/critical-security-controls/control.php?id=1))

Covered Devices

Required: Core System, Sys Admin
Recommended: Bulk Access

Threat Scenario

Attackers can discover and compromise covered data on devices not authorized to store, process, or transmit such data. If data on a device is not correctly registered, it will not receive sufficient security monitoring and appropriate prioritization of response to vulnerabilities and compromises.

Requirements

1.1 Resource Proprietors (https://security.berkeley.edu/glossary#resource-proprietor), in conjunction with Resource Custodians (https://security.berkeley.edu/glossary#resource-custodian), must register all covered Core System and Sys Admin devices in the campus data registry system (http://rdm.berkeley.edu/calnet.cfm).

1.2 Resource Proprietors and Custodians must review and update these registrations at least annually and at the time of any changes that affect registration information.

Guideline

- 1.1 Covered System Registration (https://security.berkeley.edu/node/394)
- 1.2 Registration Review (https://security.berkeley.edu/node/395)

2: Managed Software Inventory

(SANS Critical Control 2: Inventory of Authorized and Unauthorized Software (http://www.sans.org/critical-security-controls/control.php?id=2))

Covered Devices

Required: Core System, Sys Admin
Recommended: Bulk Access, Client

Threat Scenarios

Attackers use and deploy malicious software to gain unauthorized access to systems and sensitive data. When software on a device is not required for business purposes, it unnecessarily introduces potential vulnerabilities, and thereby increases the likelihood of compromise.

Requirement

2.1 Resource Custodians must manage and regularly review installed software, and install only software packages required for business purposes.

- "Manage" means:
  - Resource Custodians must utilize a process to maintain inventories of installed software packages for all devices. Inventories must include, at a minimum, detailed information about installed software, including the version number and patch level.
  - Resource Custodians must create a list of authorized software for each type of device that includes only software necessary to meet business needs.
  - The inventory process must detect and alert the Resource Custodian about unauthorized software packages discovered on a device.
- "Regularly review installed software" means:
  - A process exists for the Resource Custodian to review the list of installed software packages and reconcile that list against the authorized list of software packages. Any unauthorized software must be removed or authorized.

- "Install only software packages required for business purposes" means:
  - Software must be installed only where necessary for the business purpose or purposes for which the covered data is required.
  - Necessity must be construed narrowly, e.g., software required only for a short-term/one-time solution and not part of the standard maintenance and build of the system (such as remote administration software installed to allow a vendor to troubleshoot a problem) should be installed for that task and then promptly removed.

Additional Recommendations

- Whitelisting technology that blocks execution of unauthorized software on a device or system should be deployed.
- Software inventories should be updated on at least a monthly basis using an automated process.

Guidelines

- 2.1 Mananged Software Inventory (https://security.berkeley.edu/node/396)

3: Secure Device Configurations

(*SANS Critical Control 3: Secure Configurations for Hardware and Software on Devices (http://www.sans.org/critical-security-controls/control.php?id=3)*)

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Overly permissive default configuration settings provide an attacker with the ability to access data without authorization.

Requirement

3.1 Resource Custodians must utilize well-managed security configurations for hardware, software, and operating systems based on an industry standard.

- "Well managed" means:
  - Devices must have secure configurations in place prior to deployment.
  - Any deviations from defined security configurations must be approved through a change management process and documented. A process must exist to annually review deviations from the defined security configurations for continued relevance.
  - A process must exist to regularly check configurations of devices and alert the Resource Custodian of any changes.

Additional Recommendations

- Resource Custodians should use an automated process to regularly check configurations of laptops, workstations, and servers and send alerts based on any changes.
- Resource Custodians should follow Center for Internet Security (CIS) (https://security.berkeley.edu/node/110) platform-specific system hardening benchmarks, documenting the reasons for any variances.

Guidelines

- 3.1 Secure Device Configuration (https://security.berkeley.edu/node/397)

4: Continuous Vulnerability Assessment and Remediation

(SANS Critical Control 4: Continuous Vulnerability Assessment and Remediation (http://www.sans.org/critical-security-controls/control.php?id=4))

Covered Devices

Required: Core System, Sys Admin
Recommended: Bulk Access, Client

Threat Scenario

Attackers can discover and compromise covered data on devices that are not secured against vulnerabilities.

Requirements

4.1 Resource Custodians must continuously assess and remediate vulnerabilities on all covered devices.

"Continuously assess and remediate vulnerabilities" means:

- Automate daily vulnerability testing.
- Generate alerts and escalate visibility of critical vulnerabilities within 48 hours.
- Compare prior scans to verify that vulnerabilities are addressed.
- Report on unmitigated vulnerabilities to department and senior management.
- Measure the delay in implementing patches.

Participation in the campus vulnerability scanning program meets these requirements.

- "Participation in the campus vulnerability scanning program" means enabling all relevant firewalls to pass all IP traffic from System and Network Security (SNS) scanners. In the event a system can be disrupted by scanning, scanning exceptions can be made to alleviate the potential problem.

- "Scanning exception" means Resource Custodians block the minimum necessary to avoid the problem, and notify SNS of the block and the reason for the block. The notification is required so participation in the campus program can be adequately assessed.
- "Minimum necessary" means blocking the least amount of traffic possible to avoid the problem. For example, blocking a specific TCP port rather than all TCP traffic, or blocking a specific IP protocol rather than all IP traffic.

4.2 Resource Custodians must implement authenticated scans for vulnerability assessment for core systems. Campus-provided scanning resources and campus-licensed software may be implemented to meet this requirement.

4.3 Resource Custodians must continuously monitor for signs of attack and compromise on all covered devices.

"Continuously monitor for signs of attack and compromise" means:

- Using industry-standard network intrusion detection system (IDS) tools to analyze signatures and network behavior for signs of attack or compromise.
- Capturing at least packet headers of traffic and retain for at least 7 days, to be used as forensic data in case of a possible compromise.

Participation in the campus IDS meets this requirement.

Additional Recommendations

- Track authorized services per device.
- Route IDS data to a Security Information and Event Management system (SIEM) to correlate security events across the environment.
- Patch in a development/test environment before patching production. If patching results are unacceptable for implementation in the production environment, use other mitigation strategies to compensate for the delay in patching.
- For Sys Admin, Bulk Access, Client devices: Automated patching (e.g., TEM, Red Hat Satellite Network, Secunia, etc.)

Guidelines

- 4.1 Vulnerability Assessment and Remediation (https://security.berkeley.edu/node/398)
- 4.2 Authenticated Scans (https://security.berkeley.edu/node/399)
- 4.3 Intrusion Detection (https://security.berkeley.edu/node/400)

5: Malware Defenses

(SANS Critical Control 5: Malware Defenses (http://www.sans.org/critical-security-controls/control.php?id=5))

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Malicious software allows attackers direct access to covered data and provides attackers the means to access covered data.

Requirements

5.1 Resource Custodians must ensure that all covered devices commonly affected by malware use anti-malware defenses when anti-malware software is readily available.

- "Readily available" means the campus provides and supports a solution for a given device.

5.2 Resource Custodians must configure covered systems to not auto-run content from removable or remotely-mounted media.

Additional Recommendations

For all covered devices, Resource Custodians should:

- Use the campus-provided anti-malware solution (preferred over other solutions).
- Configure anti-malware protection to auto-scan on access.

Guidelines

- 5.1 Malware Defense (https://security.berkeley.edu/node/401)
- 5.2 Auto-Run Configuration (https://security.berkeley.edu/node/402)

6: Application Software Security

(SANS Critical Control 6: Application Software Security (http://www.sans.org/critical-security-controls/control.php?id=6))

Covered Devices

Required: Core System

Threat Scenario

Security vulnerabilities in application software allow data theft.

Requirements

6.1 Resource Proprietors and Resource Custodians must ensure that secure coding practices, including security training and reviews, are incorporated into each phase of the software development life cycle.

6.2 Resource Proprietors must ensure that web-based and other application software handling covered data passes a security assessment prior to release to production and annually thereafter.

Application security assessments must include:

- Risk evaluation criteria equivalent to the criteria used by the Campus Application Security Testing Program (https://security.berkeley.edu/node/354).
- Review of documented requirements and use cases.
- Credentialed and non-credentialed vulnerability scans conducted on a testing environment that includes web servers and databases.

Participation in the Campus Application Software Security Program meets this requirement. Resource Proprietors must obtain exception approval to substitute an alternate assessment program.

6.3 Resource Proprietors and Resource Custodians must validate that commercial software meets security criteria used by the Campus Application Security Testing Program (https://security.berkeley.edu/node/354) prior to purchase.

Guidelines

- 6.1 Secure Coding Practice (https://security.berkeley.edu/node/403)
- 6.3 Commercial Software Assessment (https://security.berkeley.edu/node/427)

7: Mobile and Wireless Device Control

(SANS Critical Control 7: Wireless Device Control (http://www.sans.org/critical-security-controls/control.php?id=7))

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Devices on insecure networks are open to multiple attack vectors. Mobile devices and removable media can be stolen or lost. Attackers can gain access to covered systems through wireless devices connected to the network.

Requirements

7.1 Resource Custodian must not implement core systems on mobile or wireless devices.

7.2 Resource Custodians must strongly encrypt covered data stored on mobile devices or removable media.

7.3 Transmission of covered data through a network must use strongly encrypted protocols.

Additional Recommendations

Covered data should not be stored on mobile or wireless devices.

Guidelines

- 7.1 No Core system on Mobilie/Wireless Devices (https://security.berkeley.edu/node/405)
- 7.2 Data Encryption at Rest (https://security.berkeley.edu/node/379)
- 7.3 Data Encryption in Transit (https://security.berkeley.edu/node/391)

8: Privacy and Security Training

(SANS Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps (http://www.sans.org/critical-security-controls/control.php?id=9))

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Regardless of implemented controls, the actions of individuals can result in the compromise of covered data.

Requirement

8.1 At least every two years, Resource Custodians, Resource Proprietors, Security Contacts, and End Users of covered data must complete privacy and security training appropriate for their role.

Additional Recommendation

System Administrators, DBA's, programmers, etc. should complete role-specific advanced training on secure practices.

Guidelines

- 8.1 Security and Privacy Training (https://security.berkeley.edu/node/406)

9: Separation of System Resources

(SANS Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services (http://www.sans.org/critical-security-controls/control.php?id=11))

Covered Devices

Required: Core System

Threat Scenario

Sharing between systems or services increases security risk. A compromise of one system can lead to a compromise of all of systems sharing the same database or credentials.

Requirements

9.1 Resource Proprietors and Resource Custodians must appropriately limit the sharing or re-use of application credentials, service accounts, user accounts, databases, and system hardware across unique systems or environments.

Additional Recommendations

Resource Proprietors and Resource Custodians should evaluate and implement the following controls where possible:

- Track a list of authorized services per device.
- Maintain and monitor a list of authorized devices.
- Segment subnets.
- Separate critical services on unique systems.

Guideline

- 9.1 Separation of System Resources (https://security.berkeley.edu/node/407)

10: Controlled Use of Administrative Privileges

(SANS Critical Control 12: Controlled Use of Administrative Privileges (http://www.sans.org/critical-security-controls/control.php?id=12))

Covered Devices

Required: Core System, Sys Admin, Bulk Access

Threat Scenario

Attackers make unauthorized use of administrative privileges to discover and compromise covered data. High risk activities increase the likelihood of introducing malicious code that takes advantage of unpatched vulnerabilities.

Requirements

10.1 Administrative credentials must be used only on devices that have been configured according to the Secure Device Configurations (https://security.berkeley.edu/mssei-2013#configurations)control.

10.2 Administrative accounts and credentials must use strong authentication, be separated from high-risk activities, and meet all requirements from the Account Monitoring and Management (https://security.berkeley.edu/mssei-2013#account) control.

- "Use strong authentication" means using passwords or passphrases that are highly resistant to persistent brute force attacks.

- "Be separated from high risk activities" means that activities at high risk of introducing malware (e.g. reading email, using a web browser, reading or editing general documents) must be separated from administrative accounts such that malware introduced through the high risk activities is not able to capture administrative passwords or read files containing private keys or other administrative credentials.

Additional Recommendation

Public/private key authentication or true two-factor authentication is strongly encouraged and is likely to be required in the future. True two-factor authentication is distinguished from other forms of strong authentication in that it requires presentation of two different categories of authentication factors (something the user knows, something the user has, and something the user is). Requiring presentation of multiple factors from the same category does not constitute multi-factor authentication.

Guidelines

- 10.1 Use of Admin Accounts on Secure Devices (https://security.berkeley.edu/node/408)
- 10.2 Admin Account Security (https://security.berkeley.edu/node/409)

11: Boundary Defense

(SANS Critical Control 13: Boundary Defense (http://www.sans.org/critical-security-controls/control.php?id=13))

Covered Devices

Required: Core System

Threat Scenario

Attackers can discover and exploit vulnerabilities in services and applications that do not need to be open to untrusted networks. A compromised system may be able to send confidential data to unauthorized systems.

Requirement

11.1 Resource Custodians must protect all core systems with a well-managed hardware firewall configured according to the principle of least privileges. These firewall rules must be reviewed annually and updated as necessary.

- “Well-managed” means:
  - All acceptable inbound and outbound traffic flows are catalogued and maintained.
  - Changes to the firewall rules go through an established approval process based on clear criteria.

    - Changes are logged and can be traced back to the request (via a ticketing system, for example).
- "Hardware firewall" means:
    - A physical network device designed to act as a stateful packet-inspecting device (i.e., it monitors the state of network connections and rejects packets not matching a known active connection). This includes network-based firewalls. If a network segment cannot support a hardware firewall or a network-based firewall is not available, a router/switch with an Access Control List may be substituted.
- "The Principle of Least Privileges" means:
    - Only traffic that is necessary is allowed through the firewall.
    - A default deny rule is set for inbound traffic with explicit allow rules for valid traffic.
    - Rules are as granular as possible, i.e., the entire campus network must not be allowed to connect to a device if only a small number of systems actually need to connect.

11.2 Resource Proprietors and Resource Custodians must implement core system devices on protected subnets.

- "Protected subnets" mean, at a minimum:
    - No implicit trusts (e.g., no access control based only on IP addresses or database access based only on user ID).
    - Physical protection from public access.
    - No wireless access points.

Additional Recommendations

- Limit allowed outbound traffic based on business requirements and implement a default deny rule for all other outbound traffic.
- Restrict outbound flows to other devices.

Guidelines

- Managed Hardware Firewall (https://security.berkeley.edu/node/410)
- Protected Subnet (https://security.berkeley.edu/node/411)

12: Audit Logging

(SANS Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs (http://www.sans.org/critical-security-controls/control.php?id=14))

Covered Devices

Required: Core System

Threat Scenario

Without appropriate audit logging, an attacker's activities can go unnoticed, and evidence of whether or not the attack led to a breach can be inconclusive.

Requirement

12.1 Resource Custodians must maintain, monitor, and analyze security audit logs for covered devices.

- "Maintain, monitor, and analyze security audit logs" means:
  - Industry-standard Security Information and Event Management (SIEM) and log correlation tools are used to analyze audit logs on all core system devices.
  - Relevant activity on core system devices (as defined by the campus Security Event Audit Logging Program) must be logged immediately.
  - Audit data must contain date, timestamp, source address, destination address, and other details about the packet.
  - All devices must use automatic time synchronization to ensure accurate time stamps for audit logs.
  - At least one full-time staff with explicit security analyst duties is responsible for daily log evaluation.
  - Device detection identifies non-responsive devices within 24 hours.

This requirement can be satisfied by participation in the campus Security Event Audit Logging Program.

Additional Recommendations

- Administrative actions on core systems should be logged. Administrative actions typically require elevated privileges such as those gained from sudo in Unix or "Run as Administrator" in Windows systems.
- Audit log information should be protected against tampering and unauthorized access.

Guidelines

- Audit Logging (https://security.berkeley.edu/node/412)

13: Controlled Access Based on the Need to Know

(SANS Critical Control 15: Controlled Access Based on the Need to Know (http://www.sans.org/critical-security-controls/control.php?id=15))

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

When access to covered data is broader than what is required for legitimate purposes, there is unnecessary risk of an attacker gaining access to the data.

Requirement

13.1 Resource Proprietors must control access to covered data and regularly review access permissions to allow use of and access to covered data only where strictly necessary for legitimate business processes.

- “Control access” means maintaining an inventory of who has access to the data and managing those accounts according to the Account Monitoring and Management (https://security.berkeley.edu/mssei-2013#account) control.
- "Regularly review access permissions" means a process exists to review individual access to covered data and to remove or modify access when there is a change in responsibilities. Review must be conducted at least annually and at defined trigger points, such as job code changes and employment terminations.

Guidelines

- 13.1 Controlled Access Based on Need to Know (https://security.berkeley.edu/node/413)

14: Account Monitoring and Management

(SANS Critical Control 16: Account Monitoring and Management (http://www.sans.org/critical-security-controls/control.php?id=16))

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Attackers can discover and exploit user accounts still valid in the system but no longer needed for business purposes.

Requirement

14.1 Resource Proprietors and Resource Custodians must manage, protect from attack, and regularly review accounts.

- “Manage” means:
  - Employ a process to grant and revoke access to accounts based on legitimate business need.
  - Access is not granted outside that process.
- “Protect from attack” means:
  - Make it difficult for non-authorized persons to access the account.
- “Regularly review” means:

- A process exists to review accounts assigned to both users and applications/services on a quarterly basis. That process validates the continued business need for each active account with the Resource Proprietor and ensures that application/service account credentials will be disabled when no longer needed.

Additional Recommendations

- Use intrusion prevention mechanisms to prevent brute force password attacks; for example, automatically block IP addresses and lock accounts upon multiple failed logins.
- Deploy two-factor authentication or CalNetKeys.

Guidelines

- 14.1 Account Monitoring and Management (https://security.berkeley.edu/node/414)

15: Data Loss Prevention

(SANS Critical Control 17: Data Loss Prevention (http://www.sans.org/critical-security-controls/control.php?id=17))

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Portable media are prone to physical theft and loss. Unauthorized parties can acquire unencrypted data stored on the device.

Requirement

15.1 Resource Custodians and anyone moving covered data through a network must use secure, authenticated, and industry-accepted encryption mechanisms.

15.2 Anyone storing covered data on removable and easily transported storage media (such as USB drives, smartphones, or CDs/DVDs) must use industry-accepted encryption technologies.

- “Industry-accepted” means accepted by the cryptographic community.

15.3 Resource Custodians must ensure that any systems (laptops, workstations, and servers) and devices (smartphones, USB drives) storing covered data must be securely overwritten or wiped using an approved secure file deletion utility upon decommission of the device to ensure that the information cannot be recovered. For those devices that cannot be overwritten (defective hard drives, CDs/DVDs), Resource Custodians must ensure the device is destroyed prior to disposal.

15.4 Resource Proprietors must establish Data Access Agreements that define appropriate use and access to covered data, as well as procedures for obtaining approval for deviance from restrictions.

Additional Recommendations

Data Access Agreements should define restrictions on access or transfer of data:

- To other persons, applications, or systems that have not independently completed an agreement for access.
- Outside the campus network, including off-site hosting, third-party vendors, and non-University email systems.
- Using removable media and unauthorized devices, including personal devices.
- Via mobile and wireless devices, and devices on networks with wireless access points.

Covered data should not be stored on any portable device (laptop, smartphone, etc.) unless absolutely necessary and if so must always be strongly encrypted.

Systems should be configured so all data written to such media are automatically encrypted without user intervention.

Guidelines

- 15.1 Data Encryption in transit (https://security.berkeley.edu/node/391)
- 15.2 Data encryption on removable media (https://security.berkeley.edu/node/379)
- 15.3 Secure Deletion (https://security.berkeley.edu/node/392)
- 15.4 Data Access Agreement (https://security.berkeley.edu/node/342)

16: Incident Response Capability

(SANS Critical Control 18: Incident Response Capability (http://www.sans.org/critical-security-controls/control.php?id=18))

Covered Devices

Required: Core System

Threat Scenario

If users and system administrators are not aware of incident response procedures, response will be delayed and evidence can be corrupted or lost, greatly increasing the potential impact of an incident.

Requirements

16.1 Each system custodian must develop and review at least annually a system-level incident response plan that contains:

- Names and contact information for the local incident response team, including:
    - Security Contact and alternate contact(s) who have system admin credentials, technical knowledge of the system, and knowledge of the location of the incident response plan.

    - A local authority/decision maker for the system who understands business impact of the system and its unavailability.
- System details, or reference to the location of such information, including:
    - Data Flow Diagrams
    - Network Diagrams
    - System hardware inventory (as required by the Annual Registration (https://security.berkeley.edu/mssei-2013#registration) control)
    - Logging information (as required by the Audit Logging (https://security.berkeley.edu/mssei-2013#logs) control)
- Procedures for reporting and handling a suspected incident, defined per role: Sys Admin, Bulk Access User, End User, e.g.,
    - Who to contact
    - How NOT to tamper with potential evidence (i.e., not to attempt forensics when not authorized).

16.2 Printed copies and/or electronic copies of the incident response plan must be accessible to all members of the local incident response team.

16.3 Resource Proprietors are responsible for training all End Users on incident reporting procedures.

Additional Recommendation

Train System Administrators and Resource Custodians on how to identify potential incidents.

Guidelines

- 16.1 Incident Response Planning (https://security.berkeley.edu/node/415)
- 16.2 Incident Response Plan Availability (https://security.berkeley.edu/node/416)
- 16.3 Incident Response Training (https://security.berkeley.edu/node/417)

17: MSSND Compliance

Covered Devices

Required: Core System, Sys Admin, Bulk Access, Client

Threat Scenario

Devices accessing data both from on-campus and off-campus are subject to attack.

Requirement

17.1 Users, Resource Proprietors and Resource Custodians must ensure that all devices accessing covered data, regardless of their location, comply with the requirements defined in the UC Berkeley Minimum Security Standard for Networked Devices

(https://security.berkeley.edu/MinStds/netdevices.html#standards) as if they were on the campus network.

Archived policy:
MSSEI_v2009_superseded.pdf
(https://security.berkeley.edu/sites/default/files/mssei_v2009_superseded.pdf)

Related Content:
Request for Exception: Berkeley Campus Minimum Security Standards
(https://security.berkeley.edu/MinStdsException.html)

Back to Top