Published on *University of Colorado* (https://www.cu.edu)

urity Standards [1]

 [2]

Information Security teams from each CU campus collaborated to develop a baseline standard that is shared across all of CU. This standard is rooted in the six core areas of the NIST Cybersecurity Framework (NIST CSF): Govern, Identify, Protect, Detect, Respond and Recover. Each CU campus builds upon this baseline standard to create broader and more detailed information security standards. Please contact your campus information security team [3] for more information on the full security standards that apply to your work.

Govern

Campus and System Administration information security programs

- Campus/System Administration information security roles and responsibilities documented (security office, IT service providers, etc.)
- A documented process exists for requesting, reviewing and approving exceptions to information security standards and processes. This process is defined in campus standards.

IT vendor information security risk management

- A process is in place to perform information security reviews of IT procurements processed through CU Marketplace

---

Identify

Data classification and inventory

- A data classification scheme is defined and is used to inform information security risk processes and decisions

Software/hardware asset management

- Campus/System Administration standards are defined for hardware and software inventory processes

---

Protect

Vulnerability management

- A Campus/System Administration level vulnerability management process is documented, including:
  - Interval for vulnerability assessments
  - Process for communicating vulnerabilities to system owners
  - Time-to-patch expectations
  - Consequences for non-compliance
- A documented, risk-based process for patch management is in place

Training and awareness

- All CU employees must complete a standard information security training module once every two years
- Standard employee information security training content is reviewed and updated at least every two years

Identity, authentication and access

- Multifactor authentication (MFA) is required on email and VPN for all users
- Users have unique accounts and single-factor authentication uses a secure method

Software development

- CU-developed code is stored in a tool that provides both access management and version control
- CU-managed public code repositories are checked for stored secrets/keys and risk-based remediations are taken

Messaging security

- Email messages are automatically scanned for malicious attachments and links, and

treated based on risk
- SPF (Sender Policy Framework) records in place with hard fail

Data protection

- Risk-based data backups and/or redundancy are in place for IT services
- Data backup and restoration processes are documented

Network security

- A default deny firewall is in place at internet border(s) with a documented process for managing policies
- Internet-facing IT services use encrypted protocols for handling and transfer of CU data (exceptions approved by ISO)

Device security (Operating system managed by CU, only applicable when the control is available for a given device)

- EDR (endpoint detection and response) is installed on all endpoints and servers, reporting to a central service and receiving updates
- Full disk encryption is used on laptop computers

Detect

Network monitoring

- Network traffic is monitored (network intrusion detection system) at internet connections
- Network security monitoring alerts are monitored and escalated to the information security incident response process as appropriate

Log monitoring

- A documented, risk-based logging standard is in place

Respond

Information security incident response process

- A documented campus level information security incident response plan is in place, covering the major phases of incident response, including lessons learned
- Incident response capabilities are in place to meet plan needs

---

Recover

Information security incident recovery

- Documented process(es) are in place for information security incident recovery

---

Groups audience:
Office of Information Security

Source URL:https://www.cu.edu/security/systemwide-baseline-security-standards

Links
[1] https://www.cu.edu/security/systemwide-baseline-security-standards
[2] https://www.cu.edu/sites/default/files/ois_sec-maturity_graphic.png [3] https://www.cu.edu/security/about