

ASU Network Security Standard

KB0028072 - v3.0 (Latest Version)

23 views



ASU Network Security Standard

Purpose

This standard will establish the process for placing and classifying assets on the ASU network. Effective implementation will minimize the risk of unauthorized access to ASU's network infrastructure, connected devices, Internet, data, computing resources, and communication systems.

Applicability

This Standard applies to all users of ASU's computing, internet, and communications resources, including all students, faculty, staff (including student employees), contractors, vendors, consultants, temporary and other workers for ASU and its Component Units (users). It also applies to networks, both logical and physical, that are owned by ASU or operated on its behalf, including on-campus and off-site cloud hosting environments.

Standard

The network security standard identifies requirements that enhance the protection against and detection of security threats to protect sensitive information managed by ASU. Baseline network standard architecture defines a 'defense in depth' strategy utilizing network zones to:

- Organize the placement of information and computing resources on the network to ensure optimal efficiency.
- Manage appropriate access to those resources.
- Enable protection and detection management of threats and attacks on those resources.

Boundary Protection

Networks with services exposed to the public Internet must be configured to deny inbound traffic by default and allow inbound network traffic by exception, following the principle of least privilege.

Firewall rules must be reviewed at a minimum every six months and restricted to the least necessary outbound traffic.

Authentication and Access Control:

Access to ASU network resources must be authenticated using a unique identity, whether human (user), device, or service. All identities accessing sensitive data or critical systems must use multi-factor authentication (MFA) or an equivalent mechanism appropriate to the identity type.

Asset Placement

Data sensitivity, application tier, and asset criticality will determine the placement of assets on the network. ASU follows a tiering model that dictates baseline security requirements for each network segment and system that reside in that segment or zone.

Additional Requirements

All network assets shall be physically protected and access controlled on a "need to access basis" per [ASU Physical Security Standard](#).

Identification and Authentication: All users and assets must be uniquely identified and authenticated before accessing ASU network resources (excluding guest networks and student networks). This includes utilizing asset inventory, network access controls, strong and complex passwords, and regularly changing passwords in accordance with ASU's password policy.

Any remote network connection to any segment other than GREEN must route all traffic through the approved secure connection tool.

Wireless networks providing access to university systems must be appropriately secured (e.g., using enterprise authentication and strong encryption such as WPA2/WPA3).

High-Risk Enterprise Devices must be attached to the network so the asset resides in a Gray Services Zone identified by ET Network Administration.

- All university and affiliate-owned assets must be registered before connecting to the campus network.

University and auxiliary affiliate-owned assets connecting to the ASU network must comply with university configuration and maintenance standards (such as anti-malware software, etc.)

Non-ASU or non-affiliate-owned assets connecting to the network must only connect to the ASU Guest Wi-Fi.

Access Control:

- Access to the ASU network must be authenticated with a unique identity, whether human (user), device, or service, with a unique identifier. Multi-factor authentication (MFA) must be implemented to access critical systems and sensitive data.
- Intrusion detection systems (IDS) and continuous network monitoring shall be in place to detect suspicious or unauthorized network activities.

Management:

- Network traffic supporting the management of networking devices must be logically segmented into a Network Management Zone. Access to the Network Management Zone is restricted to authorized devices and users for Network Management purposes.
- Network traffic is monitored for unusual or unauthorized activities or conditions at interfaces with Network Zones and the campus network border.
- FIPS-compliant encryption, such as AES-256 for VPN and TLS 1.2+ for secure web protocols, is required to transmit sensitive information.
- Sensitive data must be transported across the campus network in accordance with the [ASU Data Protection and Privacy Standard](#).
- User-initiated logical sessions will be terminated after 60 minutes of inactivity.
- All network devices shall follow the [ASU Patch Management and Vulnerability Management standard](#).
 - This requires vulnerability scanning and remediation for all network devices.
- VOIP and such services shall be managed as part of the YELLOW segment.

Special Considerations

PCI DSS

Requirement 1.2.1 Authorized and unauthorized wireless access points are managed as follows:

- The presence of Rogue wireless (Wi-Fi) access point is tested for.
- All authorized and unauthorized wireless access points are detected and identified,
- Testing, detection, and identification occur at least once every three months.

Monitoring

All network devices must record and retain audit-logging information sufficient to answer the following questions:

What activity was performed?

Who or what performed the activity, including where or on what system the activity was performed from (subject)?

- What was the activity performed on (object)?
- When was the activity performed?
- With what tool(s) was the activity performed?
- Was the activity anomalous or potentially malicious?
- What was the activity's status (such as success vs. failure), outcome, or result?
- All audit logs must be reviewed regularly and protected against unauthorized access and modification.
- Certification: Enterprise Technology will ensure that all laptops are securely and properly configured and certified before they are given out. From time to time, Users may be asked to bring their laptop into the Enterprise Technology to make sure all updates are being applied correctly and security on the laptop has not been compromised.

Policy Review and Updates

- This policy will be reviewed annually or more frequently if significant changes occur in strategic objectives, regulatory requirements, or the threat landscape.
- The Chief Information Security Officer (CISO) will lead the review, ensuring alignment with CMMC Level 1, NIST Privacy Framework, and NIST RMF controls. Recommendations for updates will be presented to senior leadership for approval, and changes will be communicated to all relevant parties.
- All reviews and updates of this policy shall follow the ASU Document Control Standard.

Violations and Enforcement

Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU's computing, Internet and communication resources, until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

Supporting Documentation and References

- [Amazon Web Services \(AWS\) Best Practices for Security, Identity, & Compliance](#)
- [Amazon Web Services \(AWS\) Security Checklist](#)
- [CIS Controls - Center for Internet Security](#)

Framework Compliance

This standard is designed to comply with:

CMMC L2	AC.L2-3.1.1 – Authorized Access Control AC.L2-3.1.3 – Control CUI Flow AC.L2-3.1.13 – Remote Access Control AC.L2-3.1.14 – Remote Access Routing (No Split Tunneling) AC.L2-3.1.16 & 3.1.17 – Wireless Access Authorization and Protection SC.L2-3.13.1 – Boundary Protection SC.L2-3.13.5 – Public System Separation SC.L2-3.13.6 – Network Communication by Exception (Default Deny) SC.L2-3.13.7 – Remote Access – No Split Tunneling SC.L2-3.13.8 – Data-in-Transit Protection SC.L2-3.13.9 – Session Disconnect SC.L2-3.13.11 – Use of FIPS-validated Encryption SC.L2-3.13.14 – VoIP and Network Services Security SC.L2-3.13.15 – Communications Authenticity AU.L2-3.3.1 – Audit Logging AU.L2-3.3.2 – Audit Log Content SI.L2-3.14.1 – Malicious Code Protection SI.L2-3.14.2 – Security Updates SI.L2-3.14.7 – Monitoring for Unauthorized Use							
	45 CFR 164.312(a)(1) – Access Control 45 CFR 164.312(b) – Audit Controls 45 CFR 164.312(c)(1) – Integrity (Protection of ePHI) 45 CFR 164.312(d) – Person or Entity Authentication 45 CFR 164.312(e)(1) – Transmission Security 45 CFR 164.312(e)(2)(i) – Integrity Controls (partial) 45 CFR 164.312(e)(2)(ii) – Encryption (partial) 45 CFR 164.310(a)(1) – Facility Access Controls (Physical Security) (partial) 45 CFR 164.308(a)(6) – Security Incident Procedures (partial) 45 CFR 164.308(a)(8) – Evaluation (Technical Evaluation) (partial)							
	16 CFR 314.4(c)(1) – Access Controls 16 CFR 314.4(c)(3) – Encryption of Customer Information (In Transit) 16 CFR 314.4(c)(8) – Monitoring and Response (Systems Monitoring) 16 CFR 314.4(b) – Risk Assessment (Identify Risks) 16 CFR 314.4(c)(5) – Multi-Factor Authentication 16 CFR 314.4(c)(2) & (4)) Secure Network Design and Asset Management							
	Article 5(1)(f) – Integrity and Confidentiality Principle Article 32(1)(a) – Encryption and Pseudonymization Article 32(1)(b) – Confidentiality, Integrity, Availability, and Resilience of Processing Systems Article 32(1)(d) – Regular Testing and Assessment Article 25(1) – Data Protection by Design and Default (partial) Article 33 – Breach Detection (Indirect Support) Article 5(2) - Accountability							
	34 CFR §99.31(a)(1)(ii) – Access Controls for Education Records FERPA Data Confidentiality							
PCI DSS	Requirement 1.1 - Processes and mechanisms for installing and maintaining network security controls are defined and understood. Requirement 1.2.1 - Network security controls (NSCs) are configured and maintained. Requirement 1.3 - Network access to and from the cardholder data environment is restricted. Requirement 1.4 - Network connections between trusted and untrusted networks are controlled. Requirement 4.1 - Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood. Requirement 8.1 - Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. Requirement 8.3 - Strong authentication for users and administrators is established and managed. Requirement 8.4 - Multi-factor authentication (MFA) is implemented to secure access to the CDE. Requirement 10.1 - Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood. Requirement 10.2 - Audit logs are implemented to support the detection of anomalies and suspicious activity and the forensic analysis of events (partial). Requirement 10.4 - Audit logs are reviewed to identify anomalies or suspicious activity (partial). Requirement 11.5 - Network intrusions and unexpected file changes are detected and responded to.							

Table A.

ASSET CRITICALITY	NETWORK SECURITY COLOR/ ZONE	SEGMENT PURPOSE	EXAMPLES	DATA SENSITIVITY	ASU STANDARDS	BU STANDARDS	SECURITY CONTROL FRAMEWORK	REVIEW & APPROVAL REQUIRED	AUDITABLE
LOW	GREEN	Resources and projects are conducted without any federal, state, or local data sensitivity and restrictions, including personally identifiable information, financial records, and export controls. Researchers may own and self-manage network and server assets. This is approved for data classified as public.	- General purpose student systems - Non-public facing desensitized resources	- Public	■				
MEDIUM	YELLOW	Business resources and projects for ASU-managed and supported systems. This segment is approved for systems that may include assets identified as critical and or data classified as both public or internal.	- General purpose business resources - Public facing resources - Critical BU resources, including BU managed	- Public - Internal	■	■		■	■
HIGH	RED	Resources and projects being conducted with sensitive data or that are under a contractual mandate to adhere to Federal requirements, information systems security control standards, or governmental regulations. This segment is approved for all levels of university classifications of data, with the exception of data that is Federally identified as Classified.	- Regulated research - Student medical records - Highly sensitive data - IAM Systems - Log Management	- Public - Internal - Sensitive - Highly Sensitive	■	■	■	■	■
**Special	Gray	Projects or research and environments with hybrid or unique security requirements that otherwise cannot follow requirements of the other color classifications.	- IoT - Honeypots - HVAC - Vendor managed equipment	- Custom	Custom	Custom	Custom	■	

ASU Confidential and Proprietary - Not for Public Release

