University of Oklahoma

Cybersecurity Policy

Policy ID:	300
Version:	1.0
Policy Owner:	Chief Information Officer (CIO)
Policy Approver:	President, University of Oklahoma

PURPOSE

Protecting University information and the systems that store, process, and transmit this information is of critical importance to the University of Oklahoma (OU). Consequently, the security of Information Systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, and availability of University information.

SCOPE

The University of Oklahoma Cybersecurity Program applies to the following:

- Information technology assets, facilities, applications, hardware systems, and network resources owned or managed by OU staff at the University of Oklahoma. This includes third party service providers' systems that access or store University data.
- All faculty and staff employed by the University, contractors, vendors and suppliers, or any other person with access to OU's network resources or Information. This includes student users and retirees.
- All categories of information, regardless of the medium, in which the Information is stored, processed, or transmitted (e.g. physical or virtual systems, cloud hosted, or mobile devices).

POLICY STATEMENTS

NETWORK MANAGEMENT

The Office of Information Technology (OU IT) is responsible for planning, implementing, and managing the University of Oklahoma network, including wireless connections. OU IT provides the following networks:

- "OU Business Networks" to include wired and wireless access provided in University Data Centers.
- "OU Campus Networks" to include wired and wireless access provided in campus buildings, facilities, and dorms for Student, Staff, and Faculty use.
- "OU Guest Networks" to include wired and wireless access provided in campus buildings or facilities, for functions unrelated to University business.
- "OU Internet Service Provider (ISP) Networks" affiliates, to include wired and wireless access provided to business partners, affiliates, or stadiums.

1. The following network devices must be registered and approved by OU IT prior to being implemented on an OU network.

Routers	Switches	Hubs
Wireless Network Devices	Firewalls	Virtual Private Networks
Intrusion Detection Devices	Intrusion Prevention Devices	Voice over IP Devices
	Consumer-grade Network Devices	

2. OU IT reserves the right to disconnect devices that are not registered appropriately and suspected of violating University Policy, compromising University data, or are exhibiting known high risk behavior.

ASSET MANAGEMENT

Asset management is critical to the University's cybersecurity strategy in understanding the assets in use at the University and their purpose.

Information System Stewards or Administrators must:

1. Maintain an inventory of physical and virtual assets supporting University missions using the instructions provided in the Procedures.
2. Categorize Information Systems into one of the following categories:
    a. Essential IT Service, defined as a service considered critical to the University and included in the University's Continuity of Operations Plan. Essential IT Services have a Maximum Tolerable Downtime of twenty-four (24) hours or less;
    b. Mission Critical Service, defined as a service considered critical to a College, Department, or Division with a Maximum Tolerable Downtime of two (2) days or less; or
    c. IT Service, defined as a service considered to be non-critical and have a Maximum Tolerable Downtime of three (3) days or more.

SYSTEM SECURITY ASSESSMENT

Technology innovations and initiatives must be brought to the attention of OU IT. System Security Assessments completed by OU IT GRC will be required upon the following events:

1. When entering into an agreement subject to DFARS 252.204-7012, an agreement requiring an Authorization to Operation (ATO), or an agreement with clauses requiring NIST SP 800-171 security controls.

2. When entering into an agreement with an entity which accepts payment on behalf of the University.
3. A System Security Assessment may be required as part of an Institutional Review Board (IRB) request if interacting with Category A – Healthcare Information.
4. A System Security Assessment may be required as part of an Institutional Data request, if sharing data with a Third Party or interconnecting more than one (1) System of Record.
5. When designing Essential IT Services, defined as a service considered critical to the University and included in the University's Continuity of Operations Plan.
6. When designing Mission Critical IT Services, defined as a service considered critical to a College, Department, or Division with dependencies upon Essential IT Services.
7. When purchasing, renewing support for, or requesting a PCard exception for any of the following types of devices:
    a. Server-Client systems interacting with:
        - Electronic Protected Health Information (ePHI)
        - Payment Card Information (PCI)
        - Family Education Rights and Privacy Act
        - Controlled Unclassified Information
        - Personally Identifiable Information (PII) data
        - University Financial Information
    b. Third Party Technology Services
    c. Medical Devices
8. The following types of devices will undergo a System Security Assessment through regular and recurring Vulnerability and any applicable Compliance scans:
    a. Web Applications or Servers
    b. Application Servers
    c. Database Servers
    d. Email Servers
    e. Network Storage Devices or File Servers
    f. Network Devices
    g. Any System or Device interacting with PCI

NOTE The System Security Risk Assessment process does not constitute an approval or authorization to purchase a reviewed product. State of Oklahoma and University purchasing rules still apply.

IDENTITY AND ACCESS MANAGEMENT

Authentication of users to IT Services must be conducted via an OU Active Directory ID and associated password. OU IT makes available the following OU ID authentication methods for use by Information Systems:

1. Single Sign-On is the preferred authentication method for applications within the OU network.
2. Microsoft Active Directory (via Windows Server) for Microsoft servers, workstations, and laptops.
3. Federated authentication.

IT Services not capable of authenticating to the OU Active Directory service (i.e., local access control mechanism), must implement access control measures commensurate to OU's Active Directory service and submit an exception at the OU IT Exception Request Page. OU IT GRC will work the requester to

evaluate the access control measures to be implemented, and facilitate the risk acceptance process, if needed.

AWARENESS AND TRAINING

Everyone is responsible for cybersecurity, making formal training and awareness programs a foundational component of any Cybersecurity Program.

1. All OU Staff, Faculty, and Students must complete annual Phishing Awareness training.
2. All OU Staff, Faculty, and Students that fail a scheduled OU IT phishing simulation must complete additional required Social Engineering Awareness training.
3. OU Staff, Faculty, or Students found to violate University Information Security Policy must complete required Information Security training to be named at the time of Incident and commensurate with the Incident type.

OU IT provides Awareness and Training content through online content, as one of the many methods for providing awareness and training materials.

DATA SECURITY

All IT Services transmitting or receiving data via public and open networks must:

1. Employ modern Secure Sockets Layer (SSL), Transport Layer Security (TLS) version 1.2 or higher, or their equivalent cryptographic protocols for authenticating and establishing identities and maintaining encrypted communications between endpoints.
2. Use a Secure Hypertext Transport Protocol (HTTPS) connection based on server-side SSL certificates signed by OU trusted Third-Party certificate provider.
3. Implement data loss protection monitoring for University endpoints in the cloud with OU's Cloud Access Security Broker (CASB), where supported.

All users transmitting data, subject to confidentiality obligations or expectations, and via email must use OU Secure Email services.

1. Users transmitting data, subject to confidentiality obligations or expectations, may use OU Secure Email services.
    - OKC/Tulsa Campus: Simply type [SECURE] in the subject line of any email message to encrypt its contents.
    - Norman/Tulsa Campus: Simply type [OUENCRYPT] in the subject line of any email message to encrypt its contents.

DEVICE MANAGEMENT

University-owned devices must be managed in order to ensure compliance with federal and/or state laws and regulations, and to align with University objectives.

1. End User devices that directly store or transmit Category A, B, C, D1, and E data types must have the OU end point management software, where supported, and installed and configured to regularly report to the centralized management server.
2. End User devices not capable of running the OU end point management software, must be reported as an IT Exception and implement sufficient mitigating controls, as described in the OU End User Device Security Policy or be operated as standalone devices with no connectivity to OU Business or Campus Networks.
3. The OU end point management service is available to IT System Administrators and includes reporting capabilities to ensure a department's compliance with University Policy and Standards.

ENCRYPTION

OU's Endpoint Encryption service leverages native encryption, such as FileVault and Bitlocker, and adds a regular device check-in to report on the status of encryption in order to protect the University against the cost of a data breach due to an unencrypted lost or stolen device. While existing native encryption provides data security, it does not provide regulatory bodies such as the Department of Education, Office for Civil Rights, and our external funding agencies with verifiable evidence that data was encrypted at the time of loss or theft.

1. OU-managed encryption must be used in accordance with the Encryption Matrix below. OU-managed encryption tools will leverage native device encryption, while providing validation of compliance with this requirement.

Figure 1 – Encryption Matrix

Category	Type	Desktop	OU Laptop	Removable Media	Cloud Service
A	Healthcare Information	**Yes**	**Yes**	**Yes**	**Yes**
B	Payment Card Information	**Yes**	**Yes**	**Yes**	**Yes**
D1	Confidential Research & Publication Information	**Yes**	**Yes**	**Yes**	**Yes**
C	Student Information	**No**	**Yes**	**Yes**	**No**
D2	Research & Publications Information	**No**	**Yes**	**Yes**	**No**
E	University Administrative & Financial Information	**No**	**Yes**	**Yes**	**No**
F	Public Information	**No**	**Yes**	**Yes**	**No**

VULNERABILITY AND PATCH MANAGEMENT

It is important to identify and install relevant patches and system updates to ensure the ongoing functionality and security of Information Systems.

1. All devices connecting to the OU Business or Campus Networks will be subject to recurring vulnerability scans.
2. Information System Administrators must remediate vulnerabilities in accordance with the Prioritization Matrix listed below or notify grc@ou.edu via e-mail if unable to remediate a vulnerability.

Figure 2 - Prioritization Matrix

Vulnerability Priority Rating (VPR)	Recommended Remediation Timeline			
	Server	End User Device	Network Device	Other
Critical	30 Days	30 Days	48 Hours	30 Days
High	60 Days	60 Days	48 Hours	60 Days
Medium	As Needed	As Needed	120 Days	As Needed
Low	As Needed	As Needed	As Needed	As Needed

MALICIOUS SOFTWARE PROTECTION

Endpoint security controls are deployed to protect end-user devices and/or secure the data sent to and from end-user devices. The OU End Point Protection software provides active protection from network threats.

1. The OU End Point Protection software provides active protection from network threats. Every University-owned device must have the OU End Point Protection software installed and configured to report to the centralized management server provided by OU IT.

REFERENCES

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Data Security Standards
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)
- National Institute of Standards and Technology Special Publication 800-171, Controlled Unclassified Information
- National Institute of Standards and Technology Special Publication 800-37, Risk Management Framework
- National Institute of Standards and Technology Cybersecurity Framework
- OU Encryption and Malicious Software Protection - Endpoint Security FAQ (Internal)
- OU Service Catalog

ENFORCEMENT AND COMPLIANCE

Failure to comply with this standard or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws. This policy is approved by the University of Oklahoma President. This Policy is enforced by the OU Chief Information Officer. Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this Policy. Such instances must be documented following the IT Policy and Standards exception process, and may require the approval of the Chief Information Officer, Chief Information Security Officer, and/or the Data Owner depending upon the level or risk introduced with the exception.

Figure 3 - Revision History

Revision Date	Version	Revised By	Changes Made
02/04/2020	0.1	OU IT, April Dickson	Baseline Version
09/22/2020	0.1	OU IT, April Dickson	Added Procedures
10/02/2020	0.2	OU IT, April Dickson	Added Enforcement & Compliance and IT Exceptions section. Revised Network Management section. Added Asset Management procedures. Added System Security Assessment procedures. Reordered the Identity and Access Management language. Added Awareness and Training procedures. Added Data Security procedures. Revised Device Management section. Revised Encryption section and added Encryption Matrix. Revised Vulnerability and Patch Management section and added Patch Management Matrix.

Figure 4 - Approval History

Version	Approval Date	Approved by:
1.0	11/10/2020	Security Governance Advisory Council
1.0	11/18/2020	Information Security Review Board
1.0	12/18/2020	University President

Figure 5 - Review History

Version	Review Date	Reviewed by:
1.0	March 2020 – October 2020	Open for Comment Period, Reviewed by Stakeholders