Acceptable Use Policy

OVERVIEW

The University of Oklahoma is committed to protecting University Personnel and the University’s University Information Systems from illegal or damaging actions by individuals.

In support of the University’s missions to provide the best possible educational experience for our students through excellence in teaching, research, and creative activity, and service to the state and society, the University provides Information and Technology Resources and services to students, faculty, staff and other entities in an atmosphere that encourages sharing of Information and open and free discussion, for academic and other purposes to support the University’s mission. Information Systems, including but not limited to University data, computer devices/equipment, software, operating systems, storage media, network resources and network accounts providing electronic mail, online browsing, and file transfer protocols (collectively, “Information Systems”), are the property of the University. These systems are to be used for business purposes in serving the interests of all University Information Systems, and of the University Information Systems clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of everyone who handles University information and Information Systems.

PURPOSE

The purpose of this Policy is to outline the acceptable use of Information Systems at all University of Oklahoma campuses. University of Oklahoma campuses include the University of Oklahoma-Norman¹, the OU Health Science Center, and the University of Oklahoma-Tulsa. These rules are in place to protect each campus’ information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction (each an “Information Security Incident”). Information Security Incidents can result in a broad range of negative consequences, including embarrassment, financial loss, non-compliance with standards and legislation and liability to third parties.

SCOPE

This Policy applies to the use of University information and/or Information Systems to conduct University business or interact with internal networks and business systems, whether owned or leased by the campus, University Personnel, or a third party.

All Individual Users are responsible for exercising reasonable judgement regarding appropriate use of University information and Information Systems in accordance with University policies and standards, and federal and state laws and regulation. Individual Users must understand they have no expectation of privacy in the use of State Information Systems and are limited to the uses as described herein.

This Policy applies to all University Personnel, of each campus, as well as third-party contractors and agents having access to University information or Information Systems controlled by the University (“Individual Users” or

¹ For purposes of this Policy, the Norman campus includes the Law Center and the Geological Survey.
POLICY STATEMENTS

100.01 GENERAL USE AND OWNERSHIP

- The University provides faculty, staff, and students with access to educational Information Systems and platforms (e.g., course management systems, learning management systems, etc.) for academic, educational, and research use. These educational systems and platforms are extensions of the classroom and learning environment. Accordingly, their use is limited to academic, educational, and research purposes. Any other use is specifically prohibited, including, but not limited to, disseminating unsolicited, commercial messages; engaging in disruptive activity or behavior; or engaging any other conduct or behavior violating a University policy. Student information (i.e., class lists, contact information, or other education records relating to students) contained on an educational Information System or platform may be used solely for participation in the course, lesson, or presentation; dissemination of such student information should adhere to University policy.

- Any University proprietary information that is stored on electronic and computing devices, whether owned or leased by the campus, the employee or a third party, remains the sole property of the campus.

- You must ensure through legal or technical means that University proprietary information is protected in accordance with this Policy.

- You are required to promptly report the theft, loss or unauthorized disclosure of University proprietary information, or any other Information Security Incident to IT Security by calling 405-271-5572.

- You may access, use or disclose University proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

- You are responsible for exercising reasonable judgement regarding the reasonableness of personal use of Information Systems.

- For security and network maintenance purposes, authorized University personnel may monitor equipment, systems and network traffic.

- University Information Systems may audit Individual Users’ use of Information Systems as permitted by applicable law on a periodic basis to ensure compliance with this Policy.

100.02 SECURITY AND PROPRIETARY INFORMATION

- All Portable Computing and Storage Devices must comply with any current University or Campus Policy, as well as applicable laws and regulations, governing Portable Computing and Storage Device Usage. See OU Information Security Policy Definitions.

- System-level and user-level passwords must comply with the OU IT Account and Password Standard. Providing access to your passwords to another individual, either deliberately or through failure to secure its access, is prohibited.

- If you use an University Information Systems email address to post to a newsgroup, forum or other group of third-party recipients, you should include a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of the campus, unless the posting is made in the course of business duties.

- You must use extreme caution when opening e-mail attachments received from unknown senders or which are otherwise not expected and suspicious, since such attachments may contain viruses and other malicious code.

- University System Security will monitor compliance with this Policy using various methods, such as business tool reports, internal and external audits, and any feedback provided to University System Security.

- University Personnel, prior to utilizing external public services for the purpose of a University mission, including instant messaging or file sharing services, must complete an OU IT System Security Assessment.

- University Personnel must only use acceptable cloud technologies for University missions. A list of acceptable cloud technologies by University mission, and based on campus, can be found at:
University of Oklahoma

Health Sciences Center
Norman Campus

*These documents are subject to change. Please check back regularly.

- University Personnel must report the following to OU IT Security immediately:
  - any event in which access to University data might have been gained by an unauthorized person
  - any event in which a device containing University information has (or might have been) lost, stolen or infected with malicious software (viruses, Trojans, etc.)
  - any event in which an account belonging to a person that has access to the data might have been compromised or the password shared with an unauthorized person (responding to phishing emails, someone shoulder surfing and writing down your password, etc.)
  - any attempt to physically enter or break into a secure area where University data is or might be stored
  - any other event in which University data has been or might have been lost or stolen
  - any event in which University information system policies, standards, or practices are violated

- University Personnel must securely dispose of hardcopy materials in accordance with the associated OU IT Information Protection Standard, based on the classification of the data being disposed of. See:
  - Category A – Healthcare Information Protection Standard
  - Category B – Payment Card Information Protection Standard
  - Category C – Education Information Protection Standard
  - Category D1 – Confidential Research and Publications Information Protection Standard
  - Category D2 – Research and Publications Information Protection Standard
  - Category E – University Administrative and Financial Information Protection Standard
  - Category F – Public Information Protection Standard

- University Personnel must mark digital and non-digital media storing Category D1 – Confidential Research and Publications Information, with necessary Controlled Unclassified Information (CUI) markings and distribution limitations in accordance with the executed contract agreements. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact discs, and digital video disks. Non-digital media includes, for example, paper and microfilm. For additional information, see OU Category D1 Confidential Research and Publications Information Protection Standard.

100.03 TRAINING

- University Personnel must complete required New Employee Orientation training within 30 days of beginning employment.
- University Personnel must acknowledge and follow the OU IT Acceptable Use Policy and OU IT Acceptable Use of Network Services Policy prior to being granted access to University Information Systems.
- University Personnel must acknowledge any additional Rules of Behavior, for Category A, Category B or Category D1 Information Systems, agreements prior to being granted access to an Information System.
- University Personnel storing, transmitting or processing Controlled Unclassified Information must complete mandatory OU CUI Program Training at least annually, and more often as necessary.
- University Personnel with a defined role in the OU IT Cybersecurity Incident Response Plan must undergo annual Cybersecurity Incident Response training.
- University Personnel with a defined role in the OU IT Disaster Recovery Plan must undergo annual Disaster Recovery training.
- University Personnel authorized for Remote Access must undergo one-time Acceptable Use of Remote Access Services training, and acknowledge the OU IT Remote Access Rules of Behavior prior to being granted access to Remote Access services.
- University Personnel who fail a scheduled OU IT phishing simulation must complete required Social
Engineering Red Flags training.

- University Personnel found to violate University Information Security Policy must complete required Information Security training.

100.04 UNACCEPTABLE USE
The activities listed below are generally prohibited. Under no circumstances is an Individual User permitted to engage in any activity that is illegal under applicable law while using University-owned resources or Information Systems. The list below is not exhaustive and provides some examples of unacceptable use.

**System and Network Activities**
The following activities are strictly prohibited without exception:

- Violating the rights of any person or University under copyright, trade secret, patent or other intellectual property laws, such as by installing or distributing “pirated” or other software products that are not appropriately licensed for use by the University.
- Accessing University information, Information Systems or a user account for any purpose other than conducting University business or as otherwise expressly permitted by University Policy.
- Importing or exporting software, technical information, encryption software or technology in violation of applicable trade laws, including export control laws. The University’s Office of Legal Counsel or Office of Export Controls should be consulted if you have any questions or concerns.
- Introducing malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) to the University’s network or server, or any other Information System.
- Revealing your account password to, or allowing use of your account by third parties. For example, you may not share your account password with family or other household members when conducting work outside of the office.
- Using any Information System to actively download or transmit material that violates applicable sexual harassment or hostile workplace laws, or otherwise violates applicable laws or regulations.
- Making fraudulent or deceptive offers of products or services originating from any University’s account.
- Making statements on the University’s behalf about the University’s representations, warranties, conditions or undertakings other than those pre-approved by the University, unless the University’s Office of Legal Counsel approval has been obtained.
- Causing or attempting to cause any security breaches, disruptions of network communications or Information Security Incidents. “Disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and using forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the Individual User's host except in accordance with University Policy.
- Circumventing user authentication protocols or the security of any host, network, account or other University or third-party system.
- Introducing honeypots, honey nets, or similar technology on the University’s network except in accordance with University Policy.
- Interfering with or disabling a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, University’s employees to parties outside of the University, except as specifically permitted by University policy.

100.05 EMAIL AND COMMUNICATION ACTIVITIES
The following activities are prohibited when using University of Oklahoma electronic messaging and communication services:
• Sending unsolicited email or other electronic messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material.
• Engaging in any form of harassment via email, telephone or text messaging, whether through the content, frequency, or size of the messages.
• Including any misrepresentations or misleading information in email header information.
• Creating or forwarding chain letters or communications relating to Ponzi, pyramid or other fraudulent or misleading schemes of any type.
• Using unsolicited electronic messages originating from within the University’s networks of other Internet/Intranet/Extranet service providers to advertise any service hosted by University Information Systems or connected via the University’s network, unless specifically authorized in writing by the University Office of Legal Counsel.
• Posting the same or similar non-business-related messages to large numbers of Individual Users or other individuals.

100.06 BLOGGING AND SOCIAL MEDIA
Limited and occasional use of the University’s Information Systems to engage in blogging and social media activities (“blogging”) is acceptable, provided that it complies with the OU Marketing and Web Communications Social Media Policy, complies with applicable laws and regulations, and does not interfere with an Individual User’s regular work duties. Blogging from University’s Information Systems may be subject to monitoring.

100.07 MONITORING
University System Security will monitor compliance with this Policy using various methods, such as business tool reports, internal and external audits, and any feedback provided to University System Security.

REFERENCES

• Healthcare Information Portability and Accountability Act (HIPAA), 45 CFR 164.308(a)(1)(ii)(B)
• Gramm-Leach-Bliley Act (GLBA), 164 CFR Part 314 section 501(b)
• Payment Card Industries (PCI) Data Security Standard version 3.2
• Family Educational Rights and Privacy Act (FERPA)
• European General Data Protection Regulation (GDPR)

ENFORCEMENT AND COMPLIANCE

Failure to comply with this policy 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 policies and laws. 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 Chief Information Officer (CIO) acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this standard. Such instances must be documented by the System Security Governance, Risk, and Compliance team at grc.ou.edu.

Table 1 Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Version</th>
<th>Revised By</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/30/2019</td>
<td>1.0</td>
<td>Sharon Nichols, GRC</td>
<td>Baseline Version</td>
</tr>
<tr>
<td>Date</td>
<td>Section</td>
<td>Author</td>
<td>Changes</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>GRC</td>
<td>Added University Personnel Awareness and Training requirements.</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>GRC</td>
<td>Added University Personnel System Security Assessment requirements.</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>GRC</td>
<td>Added University Personnel Security Incident requirements.</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>Security Governance Advisory Council</td>
<td>Added to the second paragraph of the overview section, “In support of the University's missions to provide the best possible educational experience for our students through excellence in teaching, research, and creative activity, and service to the state and society, the University provides Information and Technology Resources and services to students, faculty, staff and other entities in an atmosphere that encourages sharing of Information and open and free discussion, for academic and other purposes to support the University's mission.”</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>Security Governance Advisory Council</td>
<td>Added to line 39, “Individual Users must understand they have no expectation of privacy in the use of State Information Systems and are limited to the uses as described herein.”</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>Security Governance Advisory Council</td>
<td>Added to Section 100.10 bullet 1, “The University provides faculty, staff, and students with access to educational Information Systems and platforms (e.g., course management systems, learning management systems, etc.) for academic, educational, and research use. These educational systems and platforms are extensions of the classroom and learning environment. Accordingly, their use is limited to academic, educational, and research purposes. Any other use is specifically prohibited, including, but not limited to, disseminating unsolicited, commercial messages; engaging in disruptive activity or behavior; or engaging any other conduct or behavior violating a University policy. Student information (i.e., class lists, contact information, or other education records relating to students) contained on an educational Information System or platform may be used solely for participation in the course, lesson, or presentation; dissemination of such student information should adhere to University policy.” Replaced all instances of &quot;Institutions&quot; with University Information Systems.</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>GRC</td>
<td>Revised the Purpose section, removing “those governed by the Oklahoma Board of Regents and replacing with “The purpose of this Policy is to outline the acceptable use of Information Systems at all University of Oklahoma University Information Systems.”</td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1</td>
<td>Information Security Review Board</td>
<td>Replaced &quot;leased by an OU institution&quot; with &quot;leased by the University.&quot;</td>
</tr>
<tr>
<td>Date</td>
<td>Line(s)</td>
<td>Description and Changes</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1 Information Security Review Board</td>
<td>Modified line 65 to include &quot;to IT Security by calling 405-271-5572&quot;</td>
<td></td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1 Information Security Review Board</td>
<td>Removed from line 71 &quot;o University departments are responsible for creating Procedures concerning personal use of Information Systems. In the absence of such policies, Individual Users should be guided by departmental policies on personal use, and if there is any uncertainty, Individual Users should consult their supervisor or manager.&quot;</td>
<td></td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1 Information Security Review Board</td>
<td>Added &quot;no more than&quot; 15 minutes.</td>
<td></td>
</tr>
<tr>
<td>08/22/2019</td>
<td>1.1 Information Security Review Board</td>
<td>Replaced &quot;local, state, provincial, federal or international&quot; with &quot;applicable&quot;.</td>
<td></td>
</tr>
<tr>
<td>11/13/2019</td>
<td>1.1 GRC</td>
<td>Replaced 100.06 Social Media and Blogging statements with “Limited and occasional use of the University’s Information Systems to engage in blogging and social media activities (“blogging”) is acceptable, provided that it complies with the OU Marketing and Web Communications Social Media Policy, complies with applicable laws and regulations, and does not interfere with an Individual User's regular work duties. Blogging from University’s Information Systems may be subject to monitoring.” Language for line 95 has been revised to reflect the scope of this requirement. The new policy statement is &quot;University Personnel, prior to utilizing external public services for the purpose of a University mission, including instant messaging or file sharing services, must complete an OU IT System Security Assessment.&quot; Revised Line 77 to &quot;All Portable Computing and Storage Devices must comply with any current University or Campus Policy, as well as applicable laws and regulations, governing Portable Computing and Storage Device Usage.&quot; Removed Lines 83-85: “All Portable Computing and Storage Devices, where applicable, must be secured with a password-protected screensaver that is automatically activated after no more than 15 minutes of inactivity or less. You must lock the device's screen or log off when the device is unattended. Revised Lines 95-102: To reflect the current lists of acceptable cloud technologies. Removed Lines 123-125: “University Personnel must: o visibly wear identification badges at all times, while on premise;&quot;</td>
<td></td>
</tr>
</tbody>
</table>
record and supervise visitor and third-party support access unless previously approved.”

Removed Lines 126-129: “University Personnel must physically connect from, or disable the use of collaborative computing devices (e.g., Smart Boards, Web Cameras, Microphones, etc.) when not required to perform University business, to prevent remote activation of collaborative computing devices.”

Table 2 Approval History

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Approved by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>01/12/2020</td>
<td>Interim President, Joseph Harroz</td>
</tr>
</tbody>
</table>

Table 3 Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Review Date</th>
<th>Reviewed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>11/12/2019</td>
<td>Information Security Review Board</td>
</tr>
<tr>
<td>1.1</td>
<td>11/12/2019</td>
<td>Security Governance Advisory Council</td>
</tr>
</tbody>
</table>