Adopted: June 6, 2017
Revised:

University of Central Arkansas
Network Security Policy

Purpose:

To establish conditions for use of, and requirements for appropriate security for University Computer and Network Resources.

Scope:

This policy applies to all employees and students of the University and all University Computer and Network Resources.

Related Policies

This policy does not replace nor supercede any existing UCA policy or applicable local, state, or federal law. Policies related to this include:

- Board Policy 412
- UCA User Account Management Policy
- UCA Password Policy
- UCA Remote Access Policy
- UCA Computer Use Outside the United States Policy

Definitions

- Information Security Department - refers to the department of information security housed within the division of Information Technology at UCA.
- System Users - refers to anyone who uses any piece of technology at the University
- System Administrators - refers to any employee who is responsible for the maintenance and/or upkeep of any technology resource on campus, either directly or through management of a third party contract. System Administrators can be IT or regular UCA employees.
- University Computer and Network Resources - refers to all University-owned technology including but not limited to computers, mobile devices, servers, storage devices, cloud service accounts, email accounts, ERP systems, LMS systems, and networking equipment.

Policy:

1. Appropriate security shall include, but is not limited to: protection of the privacy of information, protection of information against unauthorized modification or disclosure, protection of systems against denial of service, and protection of systems against unauthorized access.

2. University Computer and Network Resources may be accessed or used only by individuals authorized by the University. Granting of access to a system (other than general network, myUCA, and email) must be requested by the individual's academic dean or equivalent administrative managerial personnel. Granting of access to sensitive resources must be approved by the designated UCA data owner.

3. In order to protect the security and integrity of the University Computer and Network Resources against unauthorized or improper use, and to protect authorized users from the effects of such abuse or negligence, the University reserves the rights, at its sole discretion, to limit, restrict, or terminate any account or use of Computer and Network Resources, and to inspect, copy, remove or otherwise alter any data, file, or system resources which may undermine authorized use. The University also reserves the right to inspect or check the configuration of University Computer and Network Resources for compliance with this policy, and to take such other actions as in its sole discretion it deems necessary to protect University Computer and Network Resources. The University further reserves the right to enforce these provisions without prior notice to the user.

4. The University shall not be liable for, and the user assumes the risk of, inadvertent loss of data or interference with files or processes resulting from the University's efforts to maintain the privacy, integrity, and security of the University's Computer and Network Resources.

5. Responsibilities related to access to and use of computer and network resources shall be divided among various groups. The groups listed below will be responsible for the following activities.

    a. System Users shall:

        i. understand, agree to, and comply with all University policies, security policies governing University Computer and Network Resources, and with all federal state and local laws, including laws applicable to the use of computer facilities, electronically encoded data and computer software.

        ii. safeguard passwords and/or other sensitive access control information related to their own accounts or network access. Such information must not be transmitted to, shared with, or divulged to others. Similarly, system users must recognize the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share or divulge such information, nor convert the same from encrypted or enciphered form to unencrypted form or legible text. Any attempt to conduct such actions by a system user is a violation of this policy.

iii. take reasonable precautions, including personal password maintenance and file protection measures, to prevent unauthorized use of their accounts, programs or data by others.

iv. ensure accounts or computer and network access privileges are restricted to their own use only. System users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorized computer and network access privileges to others.

v. ensure the secure configuration and operation of network services (e.g., World Wide Web, FTP, shared directories, files, and printers) they may establish on machines connected to University Computer and Network Resources.

vi. not conduct nor attempt to conduct security experiments or security probes or scans involving or using University Computer and Network Resources without the specific authorization of IT. The intentional or negligent deletion or alteration of information or data of others, intentional or negligent misuse of system resources, intentionally or negligent introduction or spreading of computer viruses, and permitting misuse of system resources by others are prohibited.

vii. respect the privacy of electronic communication. System users must not obtain nor attempt to obtain any electronic communication or information not intended for them. In particular, system users must not attempt to intercept or inspect information (e.g., packets) en route through University Computer and Network Resources, nor use University Computer and Network Resources to attempt to intercept or inspect information en route through networks elsewhere.

viii. respect the physical hardware and network configuration of University-owned networks. System users must not extend the physical network on which their system resides (e.g., wiring, jacks, wireless connection) without proper authorization.

ix. abide by all security measures implemented on University Computer and Network Resources. System users must not attempt to defeat or subvert security measures. System users must not use any other network address (e.g., IP address) for a Computer or Network Resource than has been properly assigned by an authorized system or network administrator.

x. treat non-University Computer and Network Resources in accordance with this policy. University Computer and Network Resources must not be used to attempt to breach the security or security policy of other sites (either willfully or negligently). An action or attempted action affecting non-University Computer and Network Resources that would violate this

policy if performed on University of Central Arkansas Computer and Network Resources is prohibited.

b. System Administrators shall:

(Unless otherwise stated, system administrators have the same responsibilities as system users. However, because of their position, system administrators have additional responsibilities and privileges for specific systems or networks.)

i. utilize the enterprise authentication credentials provided by IT to provide access to the System Users of each resource under their management. Exceptions to this must be authorized by IT and ISD.

ii. prepare and maintain security procedures that implement University and college/unit security policies in their local environment and that address such details as access control, backup and disaster recovery mechanisms and continuous operation in case of power outages.

iii. treat the files of system users as private. It is recognized that a system administrator may have incidental contact with system user files, including electronic mail, in the course of his or her duties. Except in the cases involving materials that violate any provision of UCA Board Policy 412, the contents of such files must be kept private. Deliberate access to system user files is authorized only under the provisions outlined in UCA Board Policy 412.

iv. take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on all systems, networks, and servers.

v. ensure that University of Central Arkansas network addresses are assigned to those entities or organizations that are part of University of Central Arkansas only. System administrators must not assign network addresses to non-University of Central Arkansas entities or organizations. System administrators may in some cases provide Domain Name Service for non-University of Central Arkansas Computer and Network Resources, but only with the approval of IT.

vi. limit access to root or privileged supervisory accounts. In general, only system administrators should have access to such accounts. System users should generally not be given unrestricted access to root or privileged supervisory accounts. As with all accounts, authorization for root or privileged supervisory accounts must be approved in accordance with this policy.

vii. take reasonable precautions to guard against corruption, compromise or destruction of Computer and Network Resources. Reasonable precautions for system administrators exceed those authorized for system users. Specifically, system administrators may intercept or inspect information en route through a network, but only for the system(s)
assigned to their supervision and only for the purposes of diagnosing and/or correcting system or network problems.

c. The Information Security Department (ISD) shall:

i. implement University-wide security policies to protect the University's Computer and Network Resources from intentional or inadvertent modification, disclosure or destruction.

ii. monitor user adherence to these policies.

iii. authorize security audits or security scans affecting Computer and Network Resources (except for those responsibilities specifically accorded to system administrators in this policy).

iv. coordinate response to computer and network security incidents to include, but not be limited to, notification of incidents to University Police, internal auditors, and other University offices as appropriate, and contact with Incident Response teams external to the University.

v. maintain methods of reporting incidents (i.e., Web forms, email addresses, emergency contact methods).

vi. require regular updates of all University Computer and Network Resource software, especially those for which demonstrated security exposures are repaired.

vii. require strong encryption and secure authentication techniques throughout all University Computer and Network Resources where possible.

viii. provide services (i.e. Web pages, FAQs, patches, virus software updates, instruction, security alerts, etc.) to assist departments and individuals to maintain security on their Computer and Network Resources.

ix. take reasonable precautions to guard against corruption, compromise or destruction of Computer and Network Resources. Reasonable precautions for ISD exceed those authorized for system users.

Specifically, ISD may conduct security scans of all UCA-owned systems. ISD may also intercept or inspect information en route through a network, but only only for purposes of security related activities or for the purposes of diagnosing system or network problems.

d. Departments and Organizations shall:

i. provide security contact information for users. This information will be maintained on the IT website.

ii. provide their employees with emergency contact information for the ISD. This information will be maintained on the ISD website.

e. Division of Information Technology (IT) shall:

i. authorize access to computer systems, including the purpose of the account, and issuance of passwords, or designating in writing the individual(s) who will exercise this responsibility for the various systems and networks within the college or administrative unit.

ii. provide enterprise authentication credentials for all University employees and students.

iii. ensure mechanisms are in place to obtain acknowledgment from System Users that they understand, and agree to comply with University security policies. Such acknowledgment must be written unless an exception is approved in accordance with the Exceptions and Exemptions section of this policy.

iv. ensure (to the best of the University's abilities) technical or procedural means are in place to facilitate determining the User ID responsible for unauthorized activity in the event of a security incident.

v. educate the user community in the ethical use of Computer and Network Resources and on best common practices and standards for implementing and improving security of Computer and Network Resources.

Copyright and Intellectual Property:

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violation using University Computer and Network Resources are prohibited. Computer software protected by copyright is not to be copied from, into, or by using University Computer and Network Resources, except as permitted by law or by the license or contract with the owner of the copyright.

Adopted: June 6, 2017
Revised:

Reporting Security Incidents or System Vulnerabilities:

Individuals aware of any breach of information or network security, or compromise of computer or network security safeguards, must report such situations to the appropriate system administrator and to the Information Security Department within 48 hours of discovery. The University Information Security Department, in coordination with appropriate University offices, will determine if financial loss has occurred and if control or procedures require modification. When warranted by such preliminary review, University Police Services, Internal Audit, and other University departments or law enforcement authorities will be contacted as appropriate.

Sanctions for Policy Violations:

Failure to comply with this policy will be investigated in accordance with UCA disciplinary procedure. Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including (but not limited to):

1. Forfeiture of University-owned device(s)
2. Suspension of network account and/or email privileges
3. Administrative disciplinary action
4. Suspension of employment with or without pay
5. Termination of employment
6. Civil action initiated by the University and/or other parties
7. Referral to appropriate law enforcement agencies

Course And Work-Related Access To Computers And Computer Networks:

Many academic course and work-related activities require the use of computers, networks and systems of the University. In the event of an imposed restriction or termination of access to some or all University computers and systems, a user enrolled in such courses or involved in computer-related work activities may be required to use alternative facilities, if any, to satisfy the obligation of such courses or work activity. However, users are advised that if such alternative facilities are unavailable or not feasible, it may be impossible to complete requirements for course work or work responsibility. The University views misuse of computers as a serious matter, and may restrict access to its facilities even if the user is unable to complete course requirements or work responsibilities as a result.

Exceptions And Exemptions

Adopted: June 6, 2017
Revised:

Exception to or exemptions from any provision of this policy must be approved by IT. Similarly, any questions about the contents of this policy, or the applicability of this policy to a particular situation should be referred to IT.