Policy Name: Acceptable Use Policy

Policy Number: 7401

.010 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment and access to the internet at University of Arkansas Grantham (University). These rules are in place to protect the employee and the University. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, and legal issues.

.020 SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct University business or interact with internal networks and business systems, whether owned or leased by the University, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at the University and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with University policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the University, including all personnel from Affiliated Organizations. This policy applies to all equipment that is owned or leased by the University.

.030 POLICY

GENERAL USE AND OWNERSHIP

University Regulated and Confidential data stored on computing devices whether owned or leased by the University, the employee or a third party, remains the sole property of the University. You must ensure through legal or technical means that Regulated and Confidential data is protected in accordance with the University's Data Classification and Security Policy.

Privacy of computing activities while using University resources is neither guaranteed nor should it be expected.

You have a responsibility to promptly report the theft, loss or unauthorized disclosure of University Regulated and Confidential data.

You have the responsibility to promptly report the theft, loss or unauthorized access of University owned physical assets.

You may access, use or share University Regulated and Confidential data only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within the University may monitor equipment, systems and network traffic at any time, per the University's security policies.

The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

SECURITY AND PROPRIETARY INFORMATION

System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Postings by employees from a University email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the University, unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

The confidentiality, security and integrity of University Data and its computing infrastructure must be maintained at all times. This obligation continues beyond the termination of the individual's relationship with the University.

UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing University owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by University.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the University or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting University business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, bots, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any University account. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior permission has been granted by the University Information Technology Department.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, University employees to parties outside the University.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages. Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the University or connected via the University's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the University".

Social media activities by employees, whether using the University's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the University's systems to engage in social media activity is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the University's policies, is not detrimental to the University's best interests, and does not interfere with an employee's regular work duties. Social media activity from University's systems is also subject to monitoring.

The University's Data Classification and Security policy also applies to social media activity. As such, Employees are prohibited from revealing any University Regulated or Confidential information, trade secrets or any other material covered by the University's Data Classification and Security policy when engaged in social media activities.

Employees shall not engage in any social media activity that may harm or tarnish the image, reputation and/or goodwill of the University and/or any of its employees. Employees are also prohibited from making any discriminatory,
disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the University's Non-Discrimination and Anti-Harassment policy.

Employees may also not attribute personal statements, opinions or beliefs to the University when engaged in social media. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the University. Employees assume any and all risk associated with their social media activity.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the University's trademarks, logos and any other University intellectual property may also not be used in connection with any social media activity.

.040 AUTHORITY AND ENFORCEMENT

Any student, staff or employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or suspension from their academic program(s).

Any student, staff or employee aware of any violation of this policy is required to report it to their supervisor, the University Compliance Department, the University Human Resources Department, or the University Information Technology Department.

.060 DEFINITIONS

Affiliated Organization - any organization associated with the University that uses university information technology resources to create, access, store or manage University Data to perform their business functions

Confidential Data - Data that is not generally available to the public but which the University is either contractually obligated to protect or the University has a need to protect.

Regulated Data – Information is classified as Regulated if protection of the information is required by law/regulation or the University is required to self-report to the government and/or provide notice to the individual if information is inappropriately accessed. If a file which would otherwise be considered to be Confidential or Unrestricted contains any element of Regulated Information, the entire file is considered to be Regulated Information.

University Data – Any data related to the University functions that are: a) stored on University information technology systems; or b) maintained by University faculty staff, or students; or c) related to institutional processes on or off campus. This applies to any format or media and is not limited to electronic data.

Social Media – Any website or online means of communication that allows for open communication and sharing on the internet including: Blogs, whether the University's own or an employee's personal one; Micro-blogging Sites such as Twitter; Online Encyclopedias such as Wikipedia; Social Networking Sites such as Facebook; and Video and photo- sharing websites such as YouTube.

.070 ROLES AND RESPONSIBILITIES

Employees are responsible for understanding and complying with all University Policies, both this policy and the other University Policies on which this policy is derived.

The Information Technology department will verify compliance to this policy through various methods, including but not limited to, business tools, reports, internal and external audits.

.090 RELATED LAWS, REGULATIONS

University Policy 7412 – Password Policy

University Policy 7435 – IT Inventory Policy

University Policy 7444 – Data Classification and Security

Policy University Policy 7485 – Copyright Compliance

Policy University Policy xxxx – Social Media Policy

University Policy xxxx – IT Security Incident Reporting Policy

University Policy xxxx – Non-Discrimination and Anti-Harassment policy

.100 QUESTIONS AND WAIVERS

The University Chief Information Officer (CIO) is responsible for this policy. The CIO or designee must approve in writing any exception to this policy.

Questions relating to this policy should be directed to the office of the CIO.

.999 REVISION HISTORY AND EFFECTIVE DATE

Below is a historical list of the revisions made to this policy.

VERSION	DATE	NOTE
1.0		n/a
2.0	2015/09/23	Updated format
3.0		Updated format