Version:	Modified By:	Date:	Approved By:	Date:
1.0	Michael Hawkins	October 29, 2013	Dan Bowden	November 2013

Rule 4-004N Payment Card Industry (PCI) Acceptable Use (proposed)

01.1 Purpose

The purpose of Acceptable Use Rule ("AUR") is intended to support the appropriate and effective use of the University of Utah ("University")'s information, systems and resources in order to protect the University and users from illegal or damaging actions by other individuals.

01.2 Scope

The AUR applies to all University personnel, contractors and temporary staff that use the University's information, systems, resources and networks.

01.3 Rule Statement

Acceptable use rules shall be documented to ensure that the University's information, systems, resources and networks are used effectively and appropriately and the University and users are protected.

1.4 Overview

The University maintains information on a variety of systems, resources and networks in a manner that complies with the University's information security policies. Access to this environment is a privilege.

The University's AUR and other information security rules/policies are not intended to abridge academic freedom, constitutional guarantees of free speech, or freedom of expression. While the rights of academic freedom and intellectual creativity are recognized, the interests of the University, students, faculty, and staff must be protected. In addition to consideration of legal liability issues, the reputation of the University is a valuable asset requiring protection.

The University's information systems, resources and networks are provided to support business activities and shall be used for those purposes. Appropriate use of information, systems and resources includes instruction, research, and the official work of the offices, departments, recognized student and campus organizations, and other agencies of the University.

Information that is stored, processed and transmitted on the University's systems, resources and networks is the property of the University. The University expects all users to use information, systems and resources in a responsible manner, respecting the rights and privacy of others, applicable laws, and the University's policies and standards.

The use of e-commerce is encouraged as a way to improve services to the University community. E-commerce systems must be used in ways conforming to the University's policies. It is critical that e-commerce systems maintain adequate security and administrative units; hosting such services safeguard the confidentiality of data related to purchases of goods and services.

1.5 Standards of Acceptable Use

All users of the University's information, systems and resources have the obligation to abide by the following standards of acceptable use:

1. Use only those information, systems, resources and networks for which you have authorization.
2. Protect the access to and integrity of information, systems, resources and networks.
3. Abide by applicable laws and the University's policies and respect the copyrights and intellectual property rights of others.
4. Use information, systems, resources and networks only for their intended purpose.
5. Respect the privacy and personal rights of others.

1.6 Acknowledgement of Security Responsibilities

All University personnel are required to confirm that they understand their information security responsibilities by acknowledging, in writing, that they agreed to the University's AUR. Users shall: [Ref: CS065, PCI, HIPAA]

1. Agree to take appropriate actions to ensure the University's information resources in their area are protected from accidents, tampering, viruses and unauthorized use or modification
2. Understand that the University has a vested interest in maintaining the integrity of copyrighted information, and shall be particularly sensitive to copyrighted information
3. Agree to handle all information stored on a computer or downloaded to portable media such as diskettes and hard copies with appropriate care to prevent unauthorized disclosure of the information
4. Agree to protect passwords and never disclose or share them with anyone
5. Agree to make passwords hard to guess by following the University's password composition standards
6. Agree to report to their supervisor any possible or actual security violations that come to their attention
7. Understand that violation of the AUR can lead to disciplinary actions
8. Agree to formally review and accept security responsibilities annually by signing the University's updated AUR

1.7 Inappropriate Use

Inappropriate use of the University's information, systems, resources and networks include:

1. Conducting illegal activities, including gambling

2. Accessing or downloading pornographic or obscene materials unless necessary for academic instruction or research
3. Soliciting for any purpose that is not explicitly approved by the University
4. Revealing or publicizing proprietary or otherwise sensitive information
5. Representing personal opinions as those of the University
6. Making or posting indecent remarks
7. Uploading or downloading commercial software in violation of its copyright
8. Utilizing the University's trademarks or logos without specific authorization from the University’s Marketing organization.
9. Downloading any software or electronic files without reasonable virus protection measures in place
10. Intentionally interfering with the normal operation of University information systems and networks
11. Attempting to bypass system security controls or gain unauthorized access
12. Attempting to undermine the security or the integrity of information systems, resources or networks
13. Intentionally damaging or disabling computer systems, networks, or software

1.8 Personal and Commercial Use

The University supports open access to electronic communication and information and members of the University community may freely communicate and access information on electronic networks, provided that the following guidelines are observed.

Personal use of information resources is permitted by the AUR. The University allows users to make reasonable and limited personal use of its electronic mail and other systems and resources.

Users must not use the University’s information systems, resources and networks to solicit business, sell products, or otherwise engage in commercial activities other than those expressly permitted by the University.

Any commercial use of the University’s information systems, resources and networks by an individual must be pre-approved. Except as authorized by the University, use of the University’s information, systems, resources and networks for personal business, political campaigning, or other commercial purposes is prohibited. The University reserves the right to prohibit personal use at any time without prior notice.

1.9 Protection of Sensitive and Restricted Information

All users must maintain the confidentiality of the University’s information. Some of the University’s Sensitive and Restricted information is protected by state, federal, and international law regarding data privacy and identity theft and must be protected accordingly. This requires users to exercise precautions that include complying with the University’s information security rules/policies.

1.10 Use of Systems and Networks

The following activities are strictly prohibited from the University’s information systems, resources and networks:

1. Effecting security breaches or disruptions of network communication. Disruptions include: network sniffing, packet floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
2. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.).
3. Port scanning, security scanning, and password cracking are expressly prohibited.
4. Performing any form of network monitoring that will intercept data not specifically intended for the user.
5. Circumventing user authentication or other security of any host, network, or account.
6. Interfering with or denying service to any user (for example, denial of service attack).
7. Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's working computer session, via any means, locally or via the Internet or network.
8. Acquiring, possessing, trading, or using hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of tools include those that defeat software copy protection, discover passwords, identify security vulnerabilities, monitor communications, or decrypt encrypted files without knowledge of the encryption key.

1.11 Use of Email

Use of the University’s electronic mail systems is permitted as long as such usage does not negatively impact the University or the user's job performance.

Email is generally considered an insecure method of communication. Sensitive or Restricted information shall not be sent via email without proper authorization, technical controls and encryption as defined in the University’s information security rules.

Users may not send any of the following types of communications:

1. Broadcast email or voice mail, without prior permission.
2. Unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
3. Any form of harassment via email, telephone or other communications system, whether through language, frequency, or size of messages.
4. Any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
5. Unauthorized use, or forging, of email header information.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. University staff and faculty shall not use personal email systems for University business.

1.12 Use of Personal Systems

Users are prohibited from connecting personally owned computer systems and devices to the University's information systems, resources and networks without explicit acceptance of the Acceptable Use Rule.

The University prohibits the attachment of personal storage media to the University's information systems, resources and networks without explicit acceptance of the Acceptable Use Rule. Prohibited storage devices include USB storage drives, external hard drives, smart phones, cameras, gaming devices, personal music/media players, and CD/DVD writers.

Non-University supplied software including games may not be stored, installed or used on any of the University's information systems, resources and networks without written permission. All software license provisions must be strictly adhered to.

1.13 Expectations of Privacy

Users shall have no expectation of privacy in anything they store, send or receive on the University's information systems, resources and networks. All information stored in and messages sent over the University's information systems and networks are subject to monitoring and review in the interest of protecting the security of the University information.

To properly maintain and manage the security of information resources, the University reserves the right to monitor and examine all information stored in or transmitted by these information systems.

1.14 Monitoring

The University actively monitors and reviews activities and content on its information systems, resources and networks. The University reserves the right to examine material stored on, processed, or transmitted through its information systems, resources and resources at any time without notice to ensure compliance with the University's policies and applicable laws.

01.15 Contacts

A. Policy Owner: Questions about this rule should be directed to the CISO, 801-213-3397 IT_policy@utah.edu

B. Policy Officer: Only the CIO, 801-581-3100, has the authority to grant exceptions to this rule.

01.16 References

A. Policy 4-002: Information Resources Policy
B. Policy 4-004: University of Utah Information Security Policy
C.

01.17 Policy Meta-Data

A. Policy Owner
B. Audience
C. Status
D. Published Date
E. Effective Date
F. Next Review Date

01.18 Revision History