14.04 Acceptable Use of Information Technology Resources

Purpose

The purpose of this policy is to outline the ethical and acceptable use of Information Technology (IT) resources at the University of Northern Iowa (UNI). These rules are in place to protect students, faculty, and staff and to ensure that members of the university community have access to reliable, robust IT resources that are safe from unauthorized or malicious use. Insecure practices and malicious acts expose UNI students, faculty, and staff to risks including malicious software, compromise of network systems and services, loss of services, and loss of data or information, including confidential data or information.

Scope

This policy applies to all faculty, staff, and students as well as any other individuals or entities who use information and IT resources at the University of Northern Iowa. This policy applies to all IT resources owned or leased by UNI and to any privately-owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, tablets, phones, multimedia devices, storage media, the campus network, and university data.

Securing and protecting these significant and costly resources from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the university community who accesses and uses IT resources.

Policy Statement

Unless otherwise specified in this policy or other university policies, use of university information technology resources is restricted to purposes related to the university's mission. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, official business with the university, and other university-sanctioned activities. Individuals may not share with or transfer to others their university accounts including network IDs, passwords, or other access codes that allow them to gain access to university information technology resources.

Colleges, departments, and other administrative units have considerable latitude in developing complementary technology use policies and procedures, as long as they are consistent with this policy and any other applicable technology use policies of the university. High-security IT resources, such as those necessary for **credit card** [1011], protected **health information** [1316], or university **Level III data,** [1409] may have strict acceptable use policies that supersede this policy.

Incidental personal use of information technology resources must adhere to all applicable university policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's university responsibilities, or adversely impact or conflict with activities supporting the mission of the university.

The university does not routinely monitor individual use of computing resources; however, all users have no expectation of privacy when using IT resources at University of Northern Iowa or when working remotely. The university reserves the right to log, access, or otherwise monitor any information stored on or passing through its systems or facilities for any business reason, without further notice or consent. Users shall not assume any personal privacy associated with personal data stored on any University of Northern Iowa systems unless such right is provided for under law or other university policy. In addition, users should be aware that electronic records may be subject to open records requirements.

Procedures

Acceptable Personal Use

Personal use of university computers and systems is restricted to incidental and emergency use. However, personal use of university Internet access on personally-owned devices may encompass any lawful use that is otherwise consistent with this and other **university policies** [317]. Staff members should be conscious of laws that provide access to public records, which includes most data located on **university IT resources** [1004].

Unacceptable Use

Users are prohibited from engaging in any activity that is illegal under local, state, federal, or international law or in violation of university policy. The following guidance is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use. The Chief Information Officer (CIO) shall have the authority to define additional unacceptable uses as new technologies or compliance requirements are adopted by the university.

Excessive Non-Priority Use of IT Resources

Priority for the use of IT resources is given to activities related to the university's missions of teaching, learning, scholarship, and outreach. University computer and network resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise appropriate restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of IT resources, such as recreational activities and non-academic, non-business services.

Unacceptable System and Network Activities

Engaging in or affecting security breaches or malicious use of network communication is an unacceptable use. This includes, but is not limited to:

- Obtaining configuration information about a network or system for which the user does not have administrative responsibility.
- Except when anonymous access is explicitly provided, engaging in activities intended to hide the user's identity or otherwise forging and/or misrepresenting the user's identity.
- Purposefully creating nuisance traffic for the network or systems attached to the network.
- Purposefully creating nuisance radio waves or Wi-Fi traffic which prevents successful wireless communication.
- Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.
- Interfering with or denying service to another user on the campus network or using university IT resources to interfere with or deny service to persons outside the university.
- Any other use that purposely causes a negative potential impact on university systems or operations or otherwise causes a loss of confidentiality, integrity, or availability of university data or services.

Unauthorized Use of Intellectual Property

Users may not use IT resources or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or **similar laws or regulations** [1003]. Violations include, but are not limited to:

- Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; and the installation, copying, or use of any copyrighted software, music, or video without an appropriate license or purchase.
- Using, displaying, or publishing licensed trademarks, including the University of Northern Iowa's trademarks, without license or authorization, or using them in a manner inconsistent with the terms of authorization.
- Exporting software, technical information, encryption software, or technology in violation of international or **regional export control laws**.
- Breaching confidentiality agreements or disclosing trade secrets or pre-publication scholarship.
- Using computing facilities and networks to engage in academic dishonesty prohibited by university policy, such as unauthorized sharing of academic work or **plagiarism**.
- Commercial use of information from university databases or university resources which is not authorized.

Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

- Setting up file sharing in which protected intellectual property is shared without permission of the rightsholder.
- Intentionally introducing malicious programs or any other computer code, files, or programs designed to interrupt, destroy, unlawfully-monitor, or limit the functionality of any computing asset, software, or communications device worldwide.
- Without appropriate approval, penetrating or attempting to penetrate security measures of the university or any other entity's computer software, hardware, network, or technical infrastructure, whether or not the intrusion affects system confidentiality, integrity, or availability.
- Conducting any port scanning, network sniffing, packet capturing, security scanning, vulnerability scanning, or any other type of network monitoring without approval.
- Inappropriate use or sharing of university-authorized IT privileges, resources, passwords, authorization, and authentication including to coworkers, family, other household members, and friends.
- Changing another user's password, access, or authorizations without approval or consent.

- Using a university IT resource to actively engage in displaying, procuring, or transmitting material that is in violation of sexual harassment, hostile workplace, or other **similar policies or laws**.
- Using any University of Northern Iowa computing asset for any private purpose and for **personal gain** to the **detriment of the State or University**, or to support a candidate or ballot measure or for **lobbying of public officials**.
- Excessive storage of personal files, such as photos, music, and movies, on university IT resources.
- Modifying or extending network services and wiring beyond their intended use.
- Intentionally denying access to data, such as by encryption, deletion, or relocation, to evade university-sanctioned monitoring, information requests, or subpoena.
- Intentionally bypassing security measures in such a manner that university data is potentially subject to a loss of confidentiality, integrity, or availability. This would include bypassing website blocks, firewalls, packet inspection, anti-virus, application whitelists, data loss prevention solutions, and other security solutions that are deployed.
- Providing confidential information to any person not authorized to have the information.

Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of the university and to individual communication among faculty, staff, students, and their correspondents. However, electronic communication must follow all university policies and should be in support of the university's mission.

Key prohibitions include:

- Sending unsolicited messages, including unsolicited commercial email ("junk mail") or other advertising material, to individuals who did not specifically request such material, except as approved under **policy 9.81 "University Communication**" or for UNI Foundation communications.
- Engaging in harassment **via electronic communications** whether through language, imagery, frequency, or size of messages.
- Masquerading as someone else by using their email address, internet address, and/or electronic signature.
- Creating or forwarding anonymous, deceptive, fraudulent, or unwelcome electronic communications, such as chain letters or solicitations for business schemes.
- Using email originating from university-provided accounts **for commercial use** or personal gain not related to University business.
- Sending or broadcasting email or other electronic communications from a university account for lobbying of public officials, or to solicit support for a candidate or ballot measure, or **otherwise using email systems** in a concerted effort to support a candidate or ballot measure.

Enforcement

The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms. The CIO may grant permission to conduct certain activities otherwise prohibited by this policy, such as for purposes related to the university's mission or to validate the confidentiality, integrity, or availability of university data.

Interim Measures

The university may temporarily disable service to an individual or a computing device, when an apparent misuse of university computing facilities or networks has occurred, and the misuse:

- Is a claim under the Digital Millennium Copyright Act (DMCA),
- Is a violation of criminal law, license agreement, or intellectual property rights,
- Has the potential to cause a loss of confidentiality, integrity, or availability of university IT resources,
- May cause significant harm to another person and/or,
- May result in liability to the university.

The person responsible for any account or equipment to be disabled as an interim measure will be informed as soon as possible so that they may present reasons why their use is not a violation or that they have authorization for the use. However, some actions may be sealed for law enforcement or court orders.

Disciplinary Action

Violations of this policy may be referred for disciplinary action as outlined in the **Student Conduct Code** [302] and applicable staff and faculty employment policies or collective bargaining agreements. The university may assess a charge to offset the cost of the incident. In extreme cases, legal action may be prudent and necessary.

Suspension of Services and Other Action

Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if:

- After hearing the user's explanation of the alleged violation, an IT Director has made a determination that the user has engaged in a violation of this policy, or
- A student or employee disciplinary body has determined that the user has engaged in a violation of the policy.

Usage of Terms

AVAILABILITY – Availability is the ability to assure that systems work promptly and service is not denied to authorized users. A loss of availability is the disruption of access to or use of information or an information system.

CONFIDENTIALITY – Confidentiality ensures that confidential information is only disclosed to authorized individuals. A loss of confidentiality, for the purposes of this policy, is the unauthorized disclosure of information.

INTEGRITY – Integrity is the appropriate maintenance of information and systems. A loss of integrity is the unauthorized modification or destruction of information.

IT RESOURCE—IT resource may include computers, software, servers, network utilization, storage utilization, virtual machine capacity, tablets, phones, multimedia devices, storage devices, wireless spectrum, and any other in-demand resource managed by IT staff.

POTENTIAL IMPACT - Potential impact is the level of adverse effect a loss of confidentiality, integrity, or availability could be expected to have on university operations, university assets, or individuals.

UNIVERSITY— University is the University of Northern Iowa.

UNIVERSITY DATA – University data are information that supports the mission and operation of the university. It is a vital asset and is owned by the university. Some university data are shared across multiple units of the university as well as outside entities.

USER—User includes any faculty, staff, student, developer, contractor, vendor, or visitor as well as any other individual or entity using information and IT resources at the University of Northern Iowa.

Office of Information Technology, approved November 29, 2016
President's Cabinet, approved February 20, 2017
President and Executive Management Team, approved February 27, 2017