Acceptable Use of Computing and Electronic Resources
Personalize with your company name and information as applicable. Be sure to check that any policies comply with local, state, and federal law.

I. Purpose

The purpose of this policy is to outline the standards for responsible and acceptable use of [company name] computer and information technology (“IT”) resources. In support of the [company name]’s mission, IT resources are provided to Authorized Users related to their [status and responsibilities] status and responsibilities to support the operations of the [company name]. Each Authorized User is expected to conduct oneself and one’s use of [company name] IT resources responsibly, ethically, in compliance with the law and the rights of one another. Inappropriate use of IT resources exposes the [company name] to risks including, but not limited to, breach of personal computer security, exposure of restricted data, compromise of network systems and services, detriments to technology performance, and legal liability.

II. Definitions

a. Information Technology Resources. IT resources include, but are not limited to, [company name] owned or leased Electronic Equipment, operating systems, storage media, applications, software, files and network accounts providing electronic mail, web browsing and file transfer.

b. Electronic Equipment. Electronic equipment includes, but is not limited to, laptop and desktop computers, tablets, mobile and smart phones, personal digital assistants, scanners, printers, flash drives, data/memory sticks and docking stations.

III. Scope

This policy applies to Authorized Users who use and/or access the IT resources whether on the [company name] worksite, or off-site through virtual personal networks. This policy applies to all equipment that is owned or leased by the [company name] and governs activity on personal devices while on the [company name] worksite that utilizes any IT resources, as well as, all communications to and from [company name] while off-site.

IV. General Use and Ownership

IT resources are the property of the [company name]. Authorized Users may use IT resources for incidental personal use and in support of the business and mission of the [company name]. It is the responsibility of each Authorized User to know and comply with this policy and security standards published by IT. This responsibility includes protecting the privacy and security of passwords, and using IT resources solely for their intended purposes. Authorized Users are solely responsible for their use of IT resources, and may not represent or imply that their associated use constitutes the views or policies of the [company name]. Communications originating from the Authorized User are identified as such and the Authorized User assumes responsibility for all communication originating from equipment or accounts assigned to that User. In the event of a security breach related to User accounts or equipment, the User shall act expeditiously to report and correct the situation.

Authorized [company name] IT personnel and/or contractors may monitor and access systems, network traffic and Electronic Equipment for maintenance, operation, security, quality of service, business-related purposes (such as audits), to investigate an alleged violation of this policy, and for policy or legal compliance. An Authorized User’s privacy will be preserved to the extent possible, subject to the [company name]’s administrative, business and legal obligations. There should be no expectation of privacy in the material sent or received when using IT resources or third party vendor applications provided by the [company name].
Unacceptable Use

The use of IT resources is a privilege, not a right. Access is granted to Authorized Users subject to all ____ and State of [state name] policies, Federal, State and local laws and ordinances. The following list, while not exhaustive, describes conduct defined as unacceptable use prohibited by this policy.

a. Knowingly using IT resources for illegal activity including, but not limited to,
   i. Sexual harassment
   ii. Discrimination on the basis of a Federally protected characteristic or sexual orientation
   iii. Intellectual property rights, including Federal copyright law, trademark, patent, trade secret or software licensing, such as pirating, installing, copying, distributing, or using digital content such as software, music text, images or video without appropriate license or as qualifies under “Fair Use”
   iv. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. Legal counsel and appropriate administration should be consulted prior to export of any material in question.
   v. Obscenity
   vi. Child pornography
   vii. Threats or harassment by means of email, instant messaging, telephone or paging, whether through language, frequency or size of messages
   viii. Defamation
   ix. Theft, including identity theft
   b. Unauthorized access, altering or reverse engineering system software or hardware configurations
   c. Disrupting, interfering with, or denying service to any Authorized User or IT service administration, including overloading or otherwise adversely impact system performance and support, regardless of whether the conduct actually impacts other Authorized Users’ use of the IT resources
   d. Access, attempted access, or facilitating access to another User’s accounts, private files, email messages, or intercepting network communication without the User’s permission, except in accordance with job responsibilities for legitimate University purposes
   e. Misrepresenting oneself as another individual electronically
   f. Any effort, regardless of whether successful, to circumvent IT system security
   g. Use for commercial gain or private profit, or personal consulting or sales
   h. Representing oneself as an agent of the ________ without authority
   i. Accessing and/or disclosing sensitive or confidential information without authority
   j. Intentionally or recklessly introducing or transmitting destructive or malicious programs such as viruses into the network or networked devices
   k. Allowing use of Authorized User’s or other accounts by others, including family and other household members
   l. Circumventing User authentication or security of any host, network or account
   m. Forwarding ________ email to unauthorized recipients
   n. Sending or posting unsolicited and/or inappropriate mass email messages without proper authorization; examples of unacceptable use include “spam” junk email, chain letters, pyramid schemes or other commercial advertising
   o. Unauthorized use, deliberate disguising of the sender, or forging of email header information, including alteration of the content of an email message originating from another sender with an intent to deceive

Enforcement

A violation of this policy constitutes unacceptable use of IT resources and may violate other ______ policies and/or federal or state law. Known or suspected violations of this policy should be reported to your supervisor or IT. _______ may suspend, block, relocate to a secure site, or restrict access to information and network resources when necessary to protect the integrity, security or functionality of IT resources or to protect the organization from liability. Authorized Users in violation of this policy may result in restriction, suspension or
termination of access to computing accounts, the network or other IT resources and/or other ______ owned technology devices as well as disciplinary action as defined in, but not limited to, the [Code of Conduct, the Employment Handbook/Personnel Manual], and other ______ policies. A violation of this policy may constitute an alleged criminal offense and may also be referred for criminal or civil prosecution under applicable Federal and/or State law(s).

VII. Review

Consistent with ________ requirements, this policy will be reviewed and updated annually or as needed based on the recommendation of IT, HR, and/or, the President/CEO.

Approved: [Date]