ACCEPTABLE USE POLICY

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS

NONE

DEFINITION OF ACCEPTABLE USE

Acceptable use defines the appropriate and responsible behavior when accessing or using {company}'s information systems, data, and technology resources. It is intended to protect the company, its employees, students, and partners from misuse, whether intentional or accidental. Only authorized users may access {company} systems, and all users are expected to act in a manner that maintains the confidentiality, integrity, and availability of information.

BY THIS POLICY

The purpose of this policy is to outline the acceptable use of computer equipment at {company}. These rules are in place to protect the students, employees and {company}. Inappropriate use exposes {company} to risks including virus attacks, compromise of network systems and services and legal issues.

APPLIES TO

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

POLICY GUIDELINES

General Use and Ownership

- Illegal activities are strictly prohibited.
- Storing personal files on servers is prohibited unless required by a current project or by the subject the user is learning.
- You may use only the computers, computer accounts and computer files for which you have authorization.
- {company} is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- Transmission of any material in violation of any international, national or state law or regulations is prohibited. This includes, but is not limited to, copyrighted materials, threatening or obscene material, harassing material or material protected by trade secrets.
- {company} proprietary information stored on electronic and computing devices whether owned or leased by {company}, the employee or a third party, remains the sole property of {company}.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of {company} proprietary information.
- You might need to sign a transfer of intellectual property rights agreement that may be used to transfer intellectual property rights from you to {university}. This form is required fairly rarely, and if you need to sign it, this will be informed separately.
- You may access, use or share {company} proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- For security and network maintenance purposes, authorized individuals within {company} may monitor equipment, systems and network traffic at any time.
- {company} reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security

- Users should store their passwords securely, should not provide passwords to others or attempt to log into any system as another user.
- Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- You shall lock the screen or log off when the device is unattended.
- Employees shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

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 are students or employees of {company} authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing {company}-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.

System and Network Activities

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 {company}.
- 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 {company} or the end user does not have an active license is strictly prohibited.

- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware and keyloggers.
- 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 {company} 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.
- 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 prohibited unless prior notification to information security manager is made.
- Executing any form of network monitoring which will intercept data.
- Circumventing user authentication or security of any host, network or account.

System and Network Activities

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 {company}.
- 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 {company} or the end user does not have an active license is strictly prohibited.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware and keyloggers.
- 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 {company} 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.
- 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 prohibited unless prior notification to information security manager is made.

- Executing any form of network monitoring which will intercept data.
- Circumventing user authentication or security of any host, network or account.

Email and Communication Activities

- 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 social media.
- Unauthorized use or forging of email header information.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Use of email to transmit materials in a manner which violates copyright laws.

POLICY COMPLIANCE

Compliance Measurement

The information security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy shall be approved by the information security manager in advance.

Non-Compliance

Students and employees found to have violated this policy may be subject to disciplinary action.

RELATED STANDARDS, POLICIES AND PROCESSES

None.

REVISION HISTORY

Version	Description	Date	Author	Approved By
1.0	Initial version	14/04/2025	ztothez	