

\*replace with your company logo

ACCEPTABLE

USE

POLICY

# Overview

\*COMPANY NAME HERE\* intention for publishing an Acceptable Use Policy is to establish a culture of openness, trust and integrity. \*COMPANY NAME HERE\* is committed to protecting its employees, partners and the \*COMPANY NAME HERE\* from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of \*COMPANY NAME HERE\*. These systems are to be used for business purposes in serving the interests of the \*COMPANY NAME HERE\*, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

1. **Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at

\*COMPANY NAME HERE\*. These rules are in place to protect the employee and

\*COMPANY NAME HERE\*.Inappropriate use exposes \*COMPANY NAME HERE\* to risks including virus attacks, compromise of network systems and services, and legal issues

## Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at \*COMPANY NAME HERE\*, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by \*COMPANY NAME HERE\*.

# Policy

### General Use and Ownership

1. While \*COMPANY NAME HERE\* network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of \*COMPANY NAME HERE\*. Because of the need to protect the \*COMPANY NAME HERE\* network, management cannot guarantee the confidentiality of information stored on any network device belonging to

\*COMPANY NAME HERE\*.

1. 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 manager.
2. It is recommended that any information that users consider sensitive

or vulnerable should be encrypted. For guidelines on information classification, see

\*COMPANY NAME HERE\* Information Sensitivity Policy.

1. For security and network maintenance purposes, authorised individuals within

\*COMPANY NAME HERE\* may monitor equipment, systems and network traffic at any time.

1. \*COMPANY NAME HERE\* reserves the right to audit networks and systems periodically to ensure compliance with this policy.
   1. **Security and Proprietary Information**
2. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: \*COMPANY NAME HERE\* private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorised access to this information.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised.
4. Postings by employees from an \*COMPANY NAME HERE\* email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of \*COMPANY NAME HERE\*, unless posting is in the course of business duties.
5. All hosts used by the employee that are connected to the \*COMPANY NAME HERE\* Internet/Intranet/Extranet, whether owned by the employee or \*COMPANY NAME HERE\*, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

# 4.3. 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 \*COMPANY NAME HERE\* authorised to engage in any activity that is illegal under local, British or international law while utilising \*COMPANY NAME HERE\*-owned resources.

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

### System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or \*COMPANY NAME HERE\* 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 NAME HERE\*.
2. Unauthorised 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 NAME HERE\* or the end user does not have an active license is strictly prohibited.
3. No data may be copied and removed from the office using a memory stick, removable disks, CDs without client permission and with the authority of a manager of

\*COMPANY NAME HERE\*.

1. 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.
2. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
3. 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.
4. Using an \*COMPANY NAME HERE\* 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.
5. Making fraudulent offers of products, items, or services originating from any

\*COMPANY NAME HERE\* account.

1. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
2. 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 authorised 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.
3. Port scanning or security scanning is expressly prohibited unless prior notification to \*COMPANY NAME HERE\* is made.
4. 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.
5. Circumventing user authentication or security of any host, network or account.
6. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
7. 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.
8. Providing information about, or lists of, \*COMPANY NAME HERE\* employees to parties outside \*COMPANY NAME HERE\*.

### Email and Communications Activities

1. 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).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of email header information.
4. 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.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within \*COMPANY NAME HERE\* networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by \*COMPANY NAME HERE\* or connected via \*COMPANY NAME HERE\* network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

# Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Definitions

### Term Definitions

Spam Unauthorised and /or unsolicited electronic mass mailing

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Note |
| 1.0 | 10/01/2021 | \*Your Name\* |  |
|  |  |  |  |