**Acceptable Use Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_a88l5gx7gbij) **4**

[**Scope**](#_sebszm58trwj) **4**

[**Policy**](#_ejfzpq5262v9) **4**

[**E-mail Use**](#_mydqr1o2qie) **4**

[**Unacceptable Use of company assets**](#_qilv8d4mcza) **4**

[**Instant Messaging**](#_vf53cxc4tpd0) **5**

[**Overuse**](#_87ruxv5pekf3) **5**

[**Web Browsing**](#_pplbfwviobtx) **5**

[**Copyright Infringement**](#_y5rltnwpsrvh) **5**

[**Remote Desktop Access**](#_qqissi7nyalb) **5**

[**Use for Illegal Activities**](#_y54ydkx51ho9) **5**

[**Disciplinary actions**](#_oo4pebgvtuk2) **6**

[**Change, Review, and Update**](#_6cu0cv3y3y7n) **6**

[**Responsibility**](#_fxvzxllev4xj) **6**

[**Reference**](#_1ksv4uv) **6**

[**Related Documents**](#_oqj2g9kzbmil) **6**

# 

# Purpose

This policy aims to describe how *[Company]* information technology resources are to be used and specifies what actions are prohibited. The purpose of this policy is to detail the acceptable use of *[Company]* information technology resources for the protection of all parties involved.

# Scope

This policy applies to all *[Company]* employees, contractors, third parties who access internal information and business processes.

# Policy

## E-mail Use

* Employees should use corporate email systems for business communications only. Personal usage of company email systems is prohibited.
* The following is never permitted, and not exhaustive: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes, forging of email header information, another person impersonation.
* Employees are not allowed to open email attachments from unknown senders or when such attachments are unexpected.

## Unacceptable Use of company assets

The user may not use the corporate network and systems to:

* Engage in activity that is illegal under country or international law.
* Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
* Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate messages or media.
* Engage in activities that cause an invasion of privacy.
* Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
* Make fraudulent offers for products or services.
* Install or distribute unlicensed or "pirated" software.
* Reveal personal or network passwords to others, including family, friends, or other household members, working from home or remote locations.

## Instant Messaging

Instant Messaging is never allowed for corporate communications, except via the following explicitly approved instant messaging platforms: Slack, Skype, Microsoft Teams, and Google Chat.

## Overuse

Actions detrimental to the computer network or other corporate resources or negatively affect job performance are not permitted.

## Web Browsing

The user should recognize this when using the Internet and understand that it is a public domain and must use the Internet at his or her own risk. The company is expressly not responsible for any information that the user views, reads, or downloads from the Internet.

## Copyright Infringement

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and unauthorized copyrighted content.

## Remote Desktop Access

Use of remote desktop software and services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited.

## Use for Illegal Activities

No company computer systems may be knowingly used for illegal activities.

Prohibited actions:

* Port scanning, security scanning, network hacking, packet sniffing, packet spoofing, denial of service, wireless hacking, keystroke logging, or other IT information gathering techniques when not part of an employee's job function.
* Act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system, terrorism.
* Identity theft or spying.
* Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes.
* Downloading, storing, or distributing copyrighted material.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how serious an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# Related Documents