# Acceptable Usage Policy

[Company Name]
Acceptable Use Policy (AUP)

Revision X.X

Responsible: [Management name]

Document Owner: [owner]

[Template:

this is a example mockup of a real world acceptable usage policy - AUP
This is subject to modification so the AUP is adjusted to the requirements to the company and comply with local law and requirement

TLP: **TLP:AMBER**

LINK DK :https://www.cfcs.dk/da/handelser/traffic-light-protocol/
LINK EN: https://www.first.org/tlp/

]

## 1. Introduction

This Acceptable Use Policy defines the principles and guidelines for the use of [Company Name]'s technology resources. This policy is designed to protect the company, its employees, partners, and customers from illegal or damaging actions by individuals, either knowingly or unknowingly..

## 2. Purpose

The primary purpose of this policy is to promote the integrity, reliability, performance, and security of [Company Name]'s technology resources. The policy aims to protect both company and personal information and to regulate the use of technology systems to reduce the risk of legal issues and security breaches.

# 3. Scope

This policy applies to all employees, contractors, interns, and temporary staff at [Company Name], as well as any external individuals or organizations accessing the company's technology resources.

# 4. Policy

## a. Use of Technology Resources:

**Work-Related Use:** Employees should use technology resources for legitimate business purposes.

**Personal Use**: Occasional personal use is permitted but should not interfere with work responsibilities.

**Prohibited Use:** Activities such as accessing inappropriate websites, excessive gaming, conducting illegal activities, or using resources for personal profit are strictly forbidden.

## b. Security and Confidentiality:

Users must respect the confidentiality and security of data they access. Unauthorized disclosure of confidential information is strictly prohibited.

**Data Protection:** Users must protect sensitive data from unauthorized access.

**Password Management:** Users should create strong passwords and change them regularly. This will be monitored and aided with a password management standard

**Incident Reporting:** Any security breaches or suspicious activities must be immediately reported to the IT department.

## c. Prohibited Activities:

Users must not engage in activities that are illegal, unethical, or harmful to the company’s reputation. This includes, but is not limited to, harassment, distributing viruses, hacking, piracy, and viewing or distributing offensive material.

**Illegal Copying**: Copying or downloading software, information, or other material in violation of copyright laws is prohibited.

**Harassment**: Using technology resources to harass, bully, or intimidate others is forbidden.

**Offensive Material:** Distributing or viewing offensive material, including pornographic, racist, or sexist content, is not allowed.

**Use of not approved software:** Software that is not approved by IT, is not allowed to be used and needs approval and test before doing so. Software not approved , is otherwise prohibited. This will be subject to monitoring in the company.

## d. Monitoring and Privacy:

[Company Name] reserves the right to monitor all activities on its technology resources for compliance with this policy. However, [Company Name] respects the privacy of its employees and will ensure that monitoring is done in a professional and lawful manner.

**Rights to Monitor**: [Company Name] reserves the right to monitor all activities on its technology resources and the right to access, review, and control data stored or transmitted.

**Privacy Expectations**: Employees should have no expectation of privacy regarding activities conducted on company-owned devices or networks. Usage of software or technology that is circumventing this, is not allowed by the company. If an employee fails to comply, this can cause termination of employment.

## e. Software Licensing and Intellectual Property:

Users must respect software licensing agreements and may not illegally copy or distribute software. Intellectual property rights must be respected.

**Compliance with Licensing:** Users must adhere to the terms and conditions of licensed software.

**Intellectual Property:** Users must respect intellectual property rights and ensure proper attribution where required.

## 5. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

- Non-compliance with this policy can result in disciplinary action, including termination and legal action.
- Employees are responsible for understanding and adhering to this policy.

You will as an employee read and understand the Acceptable Usage Policy (AUP), and sign that you have done so. In order to fulfill requirements for working in [Company Name]

## 6. Policy Review and Modification

- This policy will be reviewed annually or as needed to ensure relevance and compliance with current laws and technologies.
- Any amendments to this policy will be communicated to all employees.

## 7. Acknowledgment of Understanding

All employees, contractors, and third-party users of [Company Name] technology resources must acknowledge that they have read, understood, and agreed to abide by this policy.

[Links for further inspiration:

https://resources.workable.com/acceptable-use-policy-template
https://termly.io/resources/templates/acceptable-use-policy-template/
https://hightable.io/acceptable-use-policy/
https://www.sans.org/information-security-policy/ ]