|  |
| --- |
| **Acceptable Use Policy** |
| **Organisation:** [Organisation] |
| **Information classification:** [Category] |

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Updated by | Date | Description of changes |
| [Version Number] | [Name, Surname] | [Publish Date] |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reviewed by | Reviewer Role | Approved by | Date | To be reviewed by |
| [Name, Surname] | [Role] | [Name, Surname] | [Publish Date] | [Next Review Date] |

|  |  |  |
| --- | --- | --- |
| Document owner | An electronic copy of this document is stored at | A physical copy of this document is stored at |
| [Name, Surname] | [Location] | [Location] |

Table of contents

[1. Why should you read this document? 3](#_Toc127893808)

[2. What do we expect from you? 3](#_Toc127893809)

[2.1. Accounts and passwords 3](#_Toc127893810)

[2.2. Use of the internet 3](#_Toc127893811)

[2.3. Use of equipment 3](#_Toc127893812)

[2.3.1. General rules for handling equipment 3](#_Toc127893813)

[2.3.2. Company owned devices 4](#_Toc127893814)

[2.3.3. Personally owned devices that contain company data 4](#_Toc127893815)

[2.3.4. Personal use of professional device 4](#_Toc127893816)

[2.3.5. Physical equipment 4](#_Toc127893817)

[2.4. Company and client information 4](#_Toc127893818)

[2.5. Remote working 4](#_Toc127893819)

[2.6. Unacceptable behaviour 5](#_Toc127893820)

[2.7. Monitoring and enforcement 5](#_Toc127893821)

[3. Do you have any questions? 5](#_Toc127893822)

[Annex: Implementation checklist for the acceptable use policy statements 6](#_Toc127893823)

# Why should you read this document?

Securing our resources and data is the responsibility of all [Organisation] employees. This Acceptable Use Policy summarizes the main Information Security guidelines that should be followed within [Organisation].

The purpose of this document is to describe and explain what [Organisation] expects from its employees, how they should use the available IT resources and systems and what is expected in terms of behaviour and best practices concerning information security. Through this policy, [Organisation] can ensure the protection of employee data, ensure the continuity of activities, and minimize financial and reputational risks.

This policy is meant for all employees, consultants, and third-party contractors, who have access to [Organisation] resources, data, and information.

# What do we expect from you?

## Accounts and passwords

1. Your username and passwords of [Organisation] accounts are strictly personal and confidential. Never share or lend your credentials with/ to anyone.
2. Always use a difficult to guess password, combining upper and lower cases, numbers, and symbols.
3. Always use different passwords for personal and professional accounts.
4. Personal email should not be used for professional reasons, and vice versa.
5. If you have any suspicion that your password may be compromised, change it immediately and report it to the [Organisation IT Helpdesk].

## Use of the internet

1. If you have any suspicion that an email may be malicious, do not open it, do not download, or open the attachment and report it to [Organisation IT Helpdesk] (e.g., coming from unidentified senders or websites).
2. Respecting ethics is a fundamental pillar of [Organisation]. Do not engage or post any offensive, fraudulent, discriminatory, harassing, and obscene content.
3. Internal and confidential information shall only be shared to intended recipients through [Organisation] approved communication channels and shall only be stored on [Organisation] managed locations with appropriate access rights to prevent from unallowed access.
4. Only use cloud platforms that are approved by [IT Responsible] to store or exchange [Organisation] documents.

## Use of equipment

### General rules for handling equipment

1. You are responsible for entrusted IT equipment (e.g. laptop, smartphone) and need to protect this equipment from loss, theft and damages (e.g. key locks).
2. Lock your device when you leave it unattended.
3. Never leave any device, desktop, portable or removable media, unattended outside of the office or your home.
4. Be especially careful with removable media devices, like USB sticks. Only use [Organisation] approved devices.
5. If anything from your equipment or documents is stolen or lost, immediately report it to [Organisation IT Helpdesk].

### Company owned devices

1. Change the default password or PIN immediately when receiving a device.
2. Use Multi-Factor Authentication when feasible.
3. Always do the required security updates as soon as they are available.
4. When leaving [Organisation], return all equipment in clean, complete and functional condition.

### Personally owned devices that contain company data

1. Declare all personally owned devices used for professional purposes to [IT Responsible] before first use and familiarize yourself with minimum security requirements (e.g. installing updates, ...).
2. [IT Responsible] determines the level of network access for each personally owned device.
3. Operating systems that are no longer supported with security updates from the vendor are not allowed to process [Organisation] information.
4. Use only software downloaded from trusted sources (official app store, …) when you access the network using personally owned device.
5. Use personally owned devices with care, by among other things always doing the required security updates without undue delay and ensuring that a state of the art and up to date antivirus solution is installed.

### Personal use of professional device

1. IT equipment is entrusted to you for professional purpose.
2. A limited personal use of professional equipment is tolerated if it does not impact your work or the security of [Organisation]. This right can be revoked at any time if abuse is found.

### Physical equipment

1. Never leave confidential information unattended.
2. Entry badges are strictly personal. Never share or lend it with/ to anyone.

## Company and client information

1. Data must be processed, managed and shared in accordance with their level of confidentiality.
2. Every employee is responsible for the security of the information they are entrusted with.
3. [Organisation] and client information are strictly for professional use and cannot be used for personal gain.
4. All information acquired, created, and processed during working hours is intellectual property of [Organisation].
5. Only copy, access, modify the information you have permission and a clear business need to. If information not intended for you is disclosed, report it to [Organisation IT Helpdesk].
6. Sharing information should only be done through approved methods and channels and only with relevant recipients.
7. When in a public place, always be mindful of the surroundings when sharing information. When on the phone, don’t speak too loudly and isolate (yourself) if possible.
8. Destroy printed information as soon as it’s no longer needed by [Organisation].

## Remote working

1. Only work remotely via [Organisation] approved devices.
2. Do not use public Wi-Fi when working remotely.
3. All rules for using and handling equipment remain in force when working remotely.
4. Report immediately any suspected or confirmed security incident to [Organisation IT Helpdesk].

## Unacceptable behaviour

1. Never use [Organisation] information to obtain access to any unauthorized network or system.
2. Never deliberately edit or remove data that might impact normal business activities.
3. Never use any [Organisation] resources to engage in illegal or unethical activities.
4. Never share unauthorized, disclosed [Organisation] owned software or information.
5. Never deliberately harm intellectual property rights of others (e.g., installing cracked software, use of copyrighted images found online, ...).
6. Never install or download software against [Organisation] guidelines.

## Monitoring and enforcement

1. Be aware that in order to ensure the security of its systems and the compliance with policies, [Organisation] can monitor staff member activities to identify intentional or unintentional behaviour that may have a potential negative impact, which is in line with the [Organisation] Privacy Policy.
2. Any infraction to this policy will result in disciplinary actions according to [Organisation] procedures.

# Do you have any questions?

Always contact the [Organisation IT Helpdesk] when:

* you have any questions or remarks on this policy;
* there is any suspected or confirmed incidents.

Contact details:

* [Organisation IT Helpdesk Phone Number]
* [Organisation IT Helpdesk Email]

# Annex: Implementation checklist for the acceptable use policy statements

The table below indicates the main actions to be implemented by [Organisation]. considering the current policy. Within the “Completed?” column, the person responsible of the implementation can set the relevant status (“Yes”/”No”/”N/A”).

| Actions | Completed? |
| --- | --- |
| Ensure that all employees sign the Acceptable Use Policy before start | Choose an item. |
| Organize Awareness trainings to educate employees on the importance of this policy | Choose an item. |
| Share information according to the data classification and handling guidelines | Choose an item. |