



# Acceptable Use Policy (AUP)

Organisation: Augmentia  
Issue Date: Jul 16, 2025  
Document Owner: Alex Radcliffe

## Document Version Control

Version	Date	Description	Approver
1.0	Jul 16, 2025	Initial Release	Alex Radcliffe

## Contents

# Acceptable Use Policy (AUP)

## 1. Purpose

The purpose of this Acceptable Use Policy is to establish guidelines for the appropriate use of Augmentia's information systems, resources, and data. This policy ensures that all users are aware of their responsibilities to protect the confidentiality, integrity, and availability of information assets and to comply with applicable laws and regulations.

## 2. Scope

This policy applies to all employees, contractors, consultants, and third-party service providers who have access to Augmentia's information systems, resources, and data. It covers all computing devices, networks, applications, and data owned, leased, or controlled by Augmentia.

This policy applies to both **organisation-provided devices** and **personally owned devices (BYOD)** used to access corporate resources.

## 3. Policy Statement

Augmentia is committed to ensuring the responsible and secure use of its information systems and resources. All users are required to use these resources in a manner that is ethical, legal, and consistent with the organisation's policies and objectives.

## 4. Objectives

- Protect the confidentiality, integrity, and availability of information assets.
- Prevent misuse of information systems and resources.
- Ensure compliance with legal, regulatory, and contractual requirements.
- Promote a secure and productive work environment.

## 5. General Expectations

Users should be aware that the unauthorised disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of any Augmentia assets (physical or digital) may be subject to disciplinary action, up to and including termination of employment contract or service agreement.

It is an expectation that all Augmentia employees, contractors and other users do not act in a way that is:

- In violation of Augmentia's information security policies and procedures.
- Non-compliant with the legal and regulatory requirements placed on the organisation.
- Illegal or unethical.
- Hostile or derogatory about an individual's race, age, disability, religion, national origin, physical attributes, sexual preferences or health conditions
- Obscene or sexually explicit.
- Using Augmentia assets for non-company business or for personal gain.
- Intended to misrepresent Augmentia, its employees, or its customers.


Users who fail to adhere to this standard of behaviour will have access to assets revoked immediately and may be subject to disciplinary or legal action.

Users of Augmentia Assets must not reveal account passwords to any other user or allow use of individual accounts by others, including family and other household members when work is being done at home. Users are accountable for all the activities that are carried out using their respective login.

For security purposes, authorised individuals within Augmentia may monitor both Augmentia equipment, and devices connected to Augmentia networks, on a periodic basis, to ensure compliance with this policy.

## 6. Acceptable Use Guidelines

### General Use:

- Users must only use information systems and resources for authorised business purposes.
- Limited personal use is permitted provided it does not interfere with business operations, security, or legal compliance.
- Not circumvent the anti-malware protections installed on computers.
- Adhere to the Augmentia  **Clear Desk and Screen Policy** .

### Access Control:

- Users must not share their login credentials (usernames, passwords) with others.
- Access to information systems and data must be based on the principle of least privilege.
- Only access Augmentia systems in line with the Augmentia **Access Control Policy**.

### Data Protection:

- Users must protect sensitive and confidential information from unauthorised access and disclosure.
- Encryption must be used to protect sensitive data during storage and transmission.

### Software Use:

- Only authorised and licensed software may be installed on Augmentia devices.
- Users must not use or distribute pirated or unauthorised software.
- Use approved third party software services in a way that is consistent with third party terms of service and Augmentia policies and procedures.
- Not install or distribute "pirated" or other software products that are not appropriately licensed.
- Not engage in unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of images from copyrighted sources.
- Not install any copyrighted software for which Augmentia or the end user does not have an active licence.
- Download and install external software packages onto their computers only from known and reputable sources. Software packages from unknown sources must be authorised by the Security Officer prior to download and installation.

### Email and Communication:

- Use of email and other communication tools must be professional and related to business activities.
- Users must not send or forward chain emails, spam, or malicious content.
- Ensure all emails sent contain the Augmentia-approved email footer
- Ensure files attached to outgoing emails are protected appropriately in line with Augmentia information asset classification.
- Not engage with emails from unknown sources, or unexpected emails from known sources, in actions including but not limited to: following links and opening attachments, responding to, or forwarding such emails. These attachments may contain viruses, worms or Trojans. Any such emails must be reported to the Security Officer immediately. On no account should they be forwarded or copied to anyone, whether inside or outside the network.
- Restrict the use of group email addresses, copying to unnecessary recipients, the 'reply to all' and blind copying functions.
- Not forward emails to personal email addresses.
- Not send unsolicited email messages, including "junk mail", chain letters or other advertising material to individuals who did not specifically request such material.
- Not send defamatory emails, or use email for harassment, unauthorised purchases, or for publishing views and opinions, defamatory or otherwise about Augmentia's employees, workers, suppliers, partners or customers.
- Ensure outgoing email attachments must be appropriately protected, using cryptographic controls.
- Report any third-party email messages they receive about viruses to the Security Officer immediately.
- Limit the use of group email addresses, avoid copying Emails to unnecessary recipients, restrict use of the 'reply to all' function, and restrict the use of the blind copying feature.
- Delete non-essential e-mail messages as soon as possible and, on a regular basis, clear email boxes of correspondence that are no longer required.
- Not use Augmentia email addresses for personal purchases or any other personal transactions.
- Not set up automatic forwarding of emails to addresses external to Augmentia or of copy emails to addresses outside the organisation unless there is a legitimate business purpose for doing so.

### Internet Usage:

- Internet access must be used primarily for business-related purposes.
- Accessing, downloading, or distributing inappropriate or illegal content is strictly prohibited.
- Use approved web browsers installed on Augmentia devices as part of hardware set up.
- Not visit sites that contain obscene, hateful or sexually explicit material.
- Not make or post indecent remarks, proposals or materials on the Internet.
- Not upload, download or otherwise transmit information classified as Confidential or Restricted without the appropriate level of protection.
- Ensure that downloads from the Internet are screened for viruses before accessing.
- Not place any Augmentia material in a publicly accessible Internet site without prior approval.
- Not download software from the Internet or execute or accept any software programs or other code from the Internet unless it is in accordance with company policies and procedures.
- Not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network. Users will not examine, change or use another person's files or any other information assets for which they do not have explicit permission.
- Not carry out any other inappropriate activity as identified from time to time by Augmentia and will not waste time or Augmentia resources on non Augmentia business.

### Remote Work Security

- When working remotely, users must only connect via secure networks (e.g., VPN and company-approved Wi-Fi).
- Work should not be conducted using public or unsecured Wi-Fi networks unless a VPN is in use.
- Personal devices must have up-to-date antivirus and security patches if used for work purposes.

### Social Media and Instant Messaging

- Use social media in a responsible manner and in a way that doesn't unduly interfere with their work duties.
- Not disclose any Augmentia confidential information.
- Not behave in ways that harm the reputation of Augmentia and its stakeholders.
- Not attribute personal statements, opinions or beliefs to Augmentia.
- Not include individual Augmentia email addresses on their personal profiles.
- Not share confidential, restricted information including special category data using instant messaging apps such as Slack, Teams.

### Device Security:

- Users must ensure that devices accessing Augmentia information systems are secure and protected with up-to-date antivirus and anti-malware software.
- Lost or stolen devices must be reported immediately to the IT department.

## 7. Incident Reporting

Any suspected security incidents or breaches must be reported immediately to the IT Security Team in accordance with the Incident Management policy.

Examples of Reportable Incidents

- Phishing emails, social engineering attempts.
- Unauthorised access to company systems.
- Loss or theft of devices containing company data.
- Suspected malware infections.
- Any data leaks or inadvertent disclosure of sensitive information.

Users must cooperate with investigations and follow-up actions related to security incidents.

## 8. Training and Awareness

- All users must complete mandatory training on the Acceptable Use Policy and related information security practices.
- Regular awareness programs will be conducted to reinforce the importance of responsible use of information systems.

## 9. Review and Approval

- This Acceptable Use Policy will be reviewed annually and updated as necessary to reflect changes in technology, regulatory requirements, or the organisation's operating environment.
- The Information Security Manager will be responsible for updates and approval.
- Any significant policy updates will be communicated to all users via email and internal communication channels.

## 10. Policy Acknowledgement

All users must **acknowledge and agree to the Acceptable Use Policy** before gaining access to information systems.

- A digital acknowledgment system or a signed agreement must be used to document user acceptance.
- Failure to acknowledge the policy may result in restricted access to company resources.