SAM Assured – Acceptable Use Policy (AUP)#

Updated: 14Jan'26

Purpose

This Acceptable Use Policy ("the Policy") defines the acceptable use of SAM Assured's information systems, networks, and digital assets.
Its purpose is to protect the confidentiality, integrity, and availability of SAM Assured's data and technology resources, and to ensure compliance with applicable UK legislation, including the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

Scope

This Policy applies to:

- All **employees**, **contractors**, **consultants**, **temporary staff**, and **partners** who have access to SAM Assured systems or data.
- All company-owned or managed IT systems, including:
  - Laptops, desktops, mobile devices, and servers
  - Network resources, cloud platforms, and email systems
  - Software applications and collaboration tools (e.g., Teams, SharePoint, internal portals)

This Policy does **not** cover personal devices unless explicitly authorized under separate Bring Your Own Device (BYOD) arrangements.

Acceptable Use

Authorised users must:

- Access company systems **only for legitimate business purposes**.
- Use strong, unique passwords and maintain their confidentiality.
- Comply with all company security controls, including encryption, MFA, and access restrictions.
- Report any suspected data breach, phishing attempt, or security incident **immediately** to IT or the Information Security Manager.
- Ensure all information handled is accurate, up-to-date, and processed in line with **UK GDPR** principles.
- Log out or lock devices when unattended.

Prohibited Use

Users must **not**:

- Access, transmit, or store material that is illegal, discriminatory, defamatory, or offensive.
- Share company data or credentials with unauthorized individuals.
- Attempt to bypass or disable security mechanisms (e.g., firewalls, antivirus, access controls).
- Install unauthorized software or connect unapproved hardware to company systems.
- Use company systems for personal financial gain, external commercial activity, or political purposes.
- Copy, transfer, or process personal data outside of authorized systems or without a legitimate business purpose.

Data Protection and Privacy

- All processing of personal data must comply with **UK GDPR** and SAM Assured's **Data Protection Policy**.
- Users must handle data in accordance with the principles of **lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality**.
- Personal data must not be shared externally without prior authorisation or an appropriate legal basis (e.g., contract, consent, legitimate interest).
- Sensitive data (including client information and internal HR records) must always be stored securely and encrypted where applicable.

Monitoring and Audit

SAM Assured reserves the right to monitor, log, and audit all activity on its systems to:

- Ensure compliance with this Policy
- Investigate suspected breaches or security incidents
- Maintain operational integrity and security

Monitoring will be conducted lawfully, proportionately, and in line with the **UK GDPR** and the **Investigatory Powers Act 2016**.

Enforcement

Any breach of this Policy may result in:

- Disciplinary action up to and including termination of employment or contract
- Revocation of system access
- Legal proceedings where appropriate

Partners found in violation may have contractual arrangements suspended or terminated.