					Insert Registered Legal Entity Name Here							
Document number: P03					Document Title: **Acceptable Use Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 5	Establishes behavioural norms and requirements for the Acceptable Use Policy (AUP)
ISO/IEC 27002:2022	Controls 6.1, 6.2, 8.1, 8.12	Provides guidance on information security responsibilities, awareness, and device/data governance
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Access control and awareness/behavioural controls relevant to the use of IT assets
EU GDPR	Articles 5(1)(f), 32; Recital 39	Requires confidentiality, integrity, and availability; mandates technical and organisational controls and lawful grounds for proper use
EU NIS2	Article 21(2)(a–d)	Requires operational policies and secure use training
EU DORA	Article 5	Supports ICT risk management by regulating user behaviour
COBIT 2019	APO07, BAI05, DSS05, MEA01	Human resources, change management, managed security, and compliance/performance monitoring

1. Purpose

1.1 This policy defines the acceptable and unacceptable use of the organisation's information systems, computing resources, communication tools, and data handling practices.

1.2 It ensures that all users understand their responsibilities when using corporate IT assets and that their actions support the confidentiality, integrity, availability, and lawful processing of information.

1.3 This policy fulfils ISO/IEC 27001:2022 Clause 5.10 by establishing behavioural norms for system use and applying technical and procedural safeguards to minimise the risk of misuse, negligence, or abuse.

1.4 It also supports investigation, enforcement, and compliance activities, including incident reporting and management and disciplinary measures for violations.

2. Scope

2.1 This policy applies to all individuals and entities granted access to the organisation's information systems and assets, including but not limited to:

2.1.1 Employees, contractors, consultants, interns, and agency staff

2.1.2 External vendors with system access or delegated administrative roles

2.1.3 Guests or partners using organisation-owned or authorised IT infrastructure

2.2 The scope includes all organisational technology and data assets, including:

2.2.1 Workstations, laptops, mobile devices, and servers

2.2.2 Network infrastructure and cloud-hosted services

2.2.3 Email, messaging, file storage, collaboration platforms, and VPNs

2.2.4 Data at rest, in transit, or being processed, regardless of format or location

2.2.5 Any personal device used under a BYOD (Bring Your Own Device) arrangement that connects to organisational systems

2.3 This policy applies across all work environments, including:

2.3.1 Corporate offices and production sites

2.3.2 Remote work locations or hybrid working arrangements

2.3.3 Field-based operations or third-party-managed premises

2.4 All users must acknowledge and comply with this policy as a condition of accessing company systems or handling corporate data.

3. Objectives

3.1 To define and enforce rules for the acceptable use of organisational IT resources.

3.2 To prevent unauthorised access, data leakage, or damage resulting from negligent or malicious use.

3.3 To protect company networks, assets, and data from threats introduced through user behaviour.

3.4 To support legal and contractual obligations by demonstrating due diligence in the governance of IT resources.

3.5 To ensure consistency and clarity in the application of disciplinary actions and exception management processes.

3.6 To promote a culture of ethical, secure, and responsible use of digital and physical computing resources.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves the Acceptable Use Policy (AUP) and ensures that it aligns with business objectives, regulatory requirements, and organisational values.

4.1.2 Allocates resources for enforcement, training, monitoring, and policy review.

4.1.3 Reviews compliance status and disciplinary actions associated with policy violations as part of Information Security Management System (ISMS) governance.

4.2 IT and Information Security Teams

4.2.1 Implement technical safeguards to enforce this policy, including:

4.2.2 Content filtering, malware protection, endpoint security, and network monitoring tools

4.2.3 Email security configurations and Data Loss Prevention (DLP) solutions

4.2.4 Blocklists and allowlists for software, hardware, and websites

4.2.5 Maintain an inventory of approved and prohibited software, devices, and services.

4.2.6 Investigate suspected Acceptable Use Policy (AUP) violations, collect forensic evidence, and support disciplinary or legal action where appropriate.

4.2.7 Collaborate with Human Resources (HR) and Legal and Compliance on incident handling, escalation, and reporting obligations.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 Review Triggers and Frequency

9.1.1 This policy shall be reviewed:

9.1.1.1 At least annually

9.1.1.2 Following any significant technology or infrastructure changes

9.1.1.3 After incidents or audit findings that highlight gaps in enforcement

9.1.1.4 In response to changes in applicable laws or contracts

9.2 Ownership and Approval

9.2.1 The CISO or designated ISMS Manager is responsible for the review process.

9.2.2 Updates must be approved by Top Management and communicated across the organisation.

9.2.3 Acknowledgement of updated terms must be obtained again upon reissue of the policy.

9.3 Document Management

9.3.1 This policy must include the following metadata and version control details:

9.3.1.1 Title, ID, and classification level

9.3.1.2 Policy owner and document steward

9.3.1.3 Change history and rationale for updates

9.3.1.4 Review date and next scheduled review date

9.3.1.5 Distribution and acknowledgement log references

9.3.2 The master copy shall be retained in the ISMS Document Repository under version control.

10. Related Policies and Linkages

10.1 This policy must be interpreted in conjunction with the following:

10.1.1 P1 – Information Security Policy: Establishes the foundational behavioural expectations and senior leadership commitment to acceptable use.

10.1.2 P4 – Access Control Policy: Defines permissions and rights associated with user, system, and data access, thereby directly enforcing acceptable use boundaries.

10.1.3 P6 – Risk Management Policy: Addresses behaviour-related risks and supports monitoring and treatment activities associated with user-driven threats.

10.1.4 P7 – Onboarding and Termination Policy: Ensures acceptable use terms are acknowledged at entry and access is revoked at departure.

10.1.5 P9 – Remote Work Policy: Extends acceptable use requirements to remote and hybrid working environments.

10.2 These related policies form a defence-in-depth model for behavioural, technical, and contractual governance.

11. Reference Standards and Frameworks

11.1 This Acceptable Use Policy (AUP) is aligned with internationally recognised standards and legal frameworks to ensure enforceable, auditable, and risk-based behavioural controls across all use of digital and physical information systems.

11.2 ISO/IEC 27001:2022

11.2.1 Clause 5.10 – Acceptable Use of Information and Other Associated Assets: This policy directly fulfils the requirement to define, communicate, and enforce rules governing the appropriate use of IT resources.

11.2.2 Annex A Control 6.1 – Responsibility for Information Security: Assigns clear responsibilities for user behaviour and compliance oversight.

11.2.3 Annex A Control 6.2 – Information Security Awareness, Education, and Training: Embedded training and policy acknowledgement processes form part of Acceptable Use Policy (AUP) enforcement.

11.2.4 Annex A Control 8.1 – User Endpoint Devices and 8.12 – Data Loss Prevention: Addresses acceptable behaviour on user devices and governs activities that could lead to data exposure or leakage.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Access Control for Mobile Devices) and AC-20 (Use of External Information Systems): This policy defines user obligations and restrictions for BYOD and third-party system access.

11.3.2 PL-4 (Rules of Behaviour): Provides detailed acceptable use requirements consistent with this policy.

11.3.3 AT-2 (Security Awareness Training): Supported through user training and documented policy acknowledgement.

11.3.4 AU-2 (Audit Events) and AU-12 (Audit Generation): Enforcement relies on monitoring user actions and generating alerts for violations.

11.4 EU GDPR (2016/679):

11.4.1 Article 5(1)(f): Requires the security and integrity of personal data; this policy mitigates risks introduced by human behaviour and unauthorised use.

11.4.2 Article 32: Requires technical and organisational measures, such as behavioural controls and usage restrictions, to protect personal data.

11.4.3 Recital 39: Highlights the need to ensure that only necessary access is granted and that data is used lawfully by authorised individuals.

11.5 EU NIS2 Directive (2022/2555):

11.5.1 Article 21(2)(a–d): Requires operational policies and training for secure system use, which this Acceptable Use Policy (AUP) delivers by defining behaviour, monitoring, and enforcement processes.

11.6 EU DORA (2022/2554):

11.6.1 Article 5: This policy supports the ICT risk management framework by defining rules for human-system interaction and minimising exposure to behaviour-based cyber risk.

11.7 COBIT 2019:

11.7.1 APO07 – Manage Human Resources: Enforces user responsibilities and awareness across the employee lifecycle.

11.7.2 BAI05 – Managed Organisational Change: Embeds acceptable use governance into change processes affecting user behaviour.

11.7.3 DSS05 – Managed Security Services: Supports user activity monitoring, behavioural alerts, and automated response mechanisms.

11.7.4 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: This policy defines metrics and mechanisms to validate user compliance with behavioural expectations.