Information Security Policy

(Semi-public snapshot)

Introduction

This document defines the information security policy of Exalate.

As a modern, forward-looking business, Exalate recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Exalate has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally-recognized best practice.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Exalate systems.

Information Security Policy Areas

Exalate defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

Policy Title	**Area addressed**	**Target Audience**
Employees Code of Conduct (Acceptable Use Policy)	Business use of the information security related assets, physical facilities and uses of the internet service.	All staff
Cloud Computing Policy	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether	Users of company-provided and

	provided by the organization or the individual for business use.	BYOD (Bring Your Own Device) mobile devices
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance and equipment	Management and employees involved in setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organization's infrastructure from malware

Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All employees
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.	Employees responsible for protecting the organization's infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities

Secure Development Policy	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All employees
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data

Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media	All employees

exalate