#Company_Name#

INFORMATION SECURITY-POLICY

1 Purpose

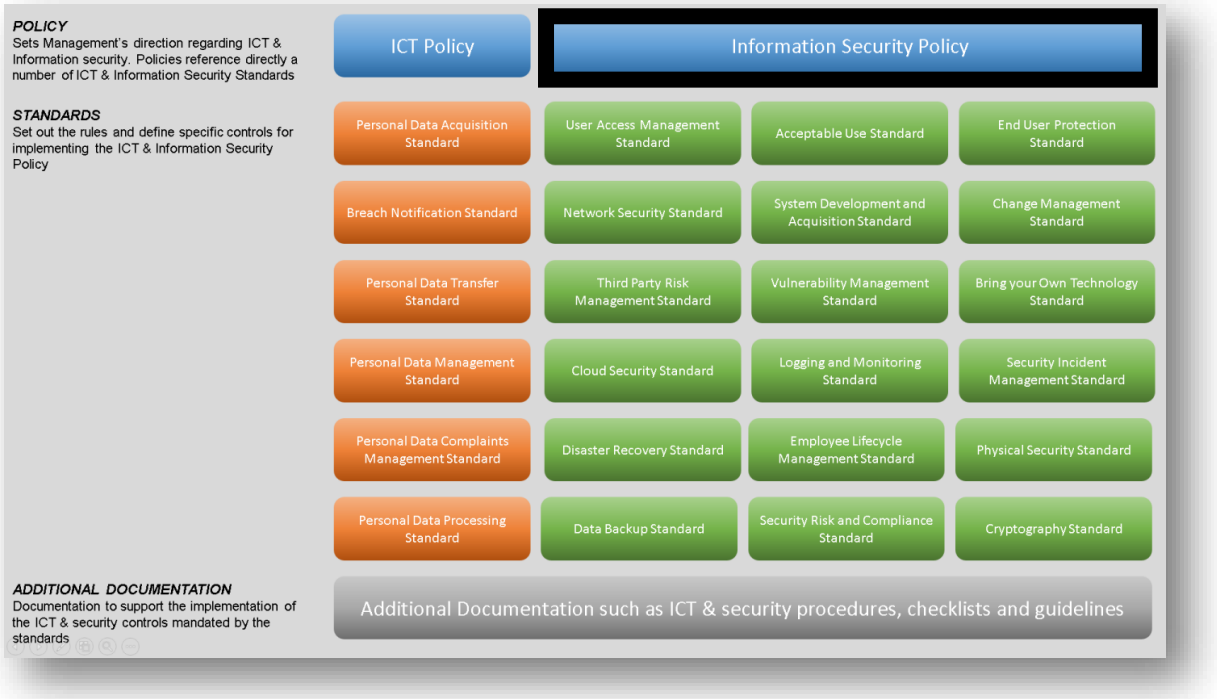
The Information Security Policy (ISP) sets out the information security direction and is the backbone of our information security posture. The aim of this policy is to proactively and actively identify, mitigate, monitor and manage information security threats and risks.

The purpose of this policy is to ensure that our information can be used when required with the confidence that it is accurate, complete and adequately protected from misuse, unauthorized disclosure, damage or loss.

1.1 Document Context

This policy is the backbone of our Information Management Framework (IMF). The IMF provides structure to the development and maintenance of ICT and security controls to actively manage, operate and secure our information assets from information security threats and ICT risks.

The IMF's structure is depicted in this diagram.



2 Application

This policy and the obligations imposed by the Code of Conduct apply not only to employees of our company (whether permanent, fixed or temporary, and including directors, executives and leaders), but also any third party or sub-contractor providing services to us. In this policy, the term employee includes all these groups.

This policy is applicable to our information assets used to provide and support our business operations.

'We', 'us' and 'our' shall mean all related bodies corporate of #Company_Name#.

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

3 Policy Statements

3.1 User Access Management

User access requests (e.g. adding new users, updating access privileges and revoking user access rights) must be logged, assessed and approved in accordance with defined user access management procedures.

See "User Access Management Standard"

3.2 Security Incident Management

Incident detection mechanisms such as security event logging and anti-virus applications must be implemented for our IT systems. Potential security incidents must be handled appropriately following formalized security incident handling procedures.

See "Security Incident Management Standard"

3.3 Information Classification and Handling

Our IT assets (hardware and software) must be recorded in an inventory which must be kept updated always. Our IT assets must be classified and handled according to their criticality.

See "Information Classification and Handling Standard"

3.4 Vulnerability Management

Security patch and vulnerability management processes must be in place to identify, prioritized and remediate security vulnerabilities on our IT assets.

See "*Vulnerability* Management Standard"

3.5 Data Backup

Data must be backed up on a regular basis, protected from unauthorized access or modification during storage and available to be recovered in a timely manner in the event of incident or disaster.

See "Data Backup Standard"

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

3.6 Logging and Monitoring

Key security-related events, such as user privilege changes, must be recorded in logs and protected against unauthorized changes. Logs must be analyzed on a regular basis to identify potential unauthorized activities and facilitate appropriate follow-up action.

See “Logging and Monitoring Standard”

3.7 Cloud Security

Cloud services must only be utilized following a formalized risk assessment to identify the necessary security controls that must be established by the Cloud Service Provider and us to manage security risks to an acceptable level.

See “Cloud Security Standard”

3.8 Network Security

Our network architecture must be commensurate with current and future business requirements, as well as emerging security threats. Appropriate controls must be established to ensure security of our data in private and public networks and to protect IT services from unauthorized access.

See “Network Security Standard”

3.9 IT System Acquisition & Development

IT security requirements must be addressed, within the software development lifecycle, to reduce the risk of vulnerabilities being introduced during the acquisition or development of IT systems. A “defense in depth” strategy must be followed when developing our internet-facing (Web) applications.

See “IT System Acquisition & Development Standard”

3.10 Change Management

Change requests must be promptly and efficiently assessed for potential security risks. The requirements, risk and impact of each request must be evaluated and the proposed risk mitigation solution must be documented and approved.

See “Change Management Standard

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

3.11 Cryptography

Cryptography must be used for protecting sensitive data during its transmission and storage. Data masking must be used to obscure (mask) sensitive information in non-production environments. For GDPR compliance Pseudonymisation is used to provide a separation between the PII and the personal data.

See “Cryptography Standard”

3.12 Physical Security

The facilities (e.g. data centers, computer rooms, etc.), where critical information is stored or processed, must be constructed and arranged in a way that data is adequately protected from physical and environmental threats.

See “Physical Security Standard”

3.13 Bring Your Own Technology (BYOT)

Our employees connecting personally owned devices to our networks must be subject to specific restrictions to protect our IT environment and data.

See “Bring Your Own Technology Standard”

3.14 IT Acceptable Use

Our users having access to our IT systems and services must adhere to specific rules regarding the use of our IT systems and/or services.

See “IT Acceptable Use Standard”

3.15 Disaster Recovery Standard

A Disaster Recovery Plan, and relative procedures, must be in place to enable the recovery of our business-critical services in a timely manner to minimize the effect of IT disruptions and maintain resilience, before, during and after a disruption.

See “Disaster Recovery Standard”

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

3.16 Information Security Risk & Compliance Management

Information security risk must be identified, mitigated and monitored through formalized risk management procedures. Compliance with our information security standards must be measured and monitored.

See “Information Security Risk and Compliance Standard”

3.17 Third Party Risk Management

Security risks arising from our contracted third parties (i.e. suppliers, vendors etc.), who maintain direct or indirect access to our systems and data, must be operationally and contractually controlled.

See “Third Party Risk Management Standard”

3.18 Employee Lifecycle Management

Our staff and contractors must be subject to specific security processes before, during, and after the termination of their employment or contract.

See “Employee Lifecycle Management Standard”

3.19 End User Protection

Our end user desktop computers, mobile computers (e.g. laptops, tablets, etc.), as well as portable computing devices (e.g. portable hard drives, USB memory sticks, etc.), must be protected with adequate security mechanisms to prevent the unauthorized disclosure and/or modification of our data.

See “End User Protection Standard”

4 Governance

4.1 Review of Information Security Policy

The Information Security Policy (ISP) (and the Information Security Standards) must be reviewed on an annual basis to ensure that they remain appropriate to our needs. In addition to the pre-defined review, our Information Security Policy needs to continuously evolve to meet changing internal and external requirements, which may include:

- changes to our business and IT environment or tolerance to risk;

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

- changes to regulatory requirements;
- changes to contractual requirements, and;
- changes to adapt to emerging risks and threats.

4.2 Handling Exemptions to Information Security Policy and Standards

The Control Exception Process set out in our exception processes allows our business units (where technological or operational constraints or a legitimate business requirement exists) to request an exception from a defined control within the Information Security Policy and/or Information Security Standards. Exemptions requests must be reviewed and assessed by the Information Security Risk and Governance Manager and the Data Protection Officer and approved by the Chief Information Officer.

5 Definitions

For definitions and information relating to key terms and acronyms referred to in this Policy or the Information Security Standards please refer to the Information Management Framework Glossary.

6 Related documents

Document	Version	Location
User Access Management Standard	1.0	#2_2_Location#
Vulnerability Management	1.0	#4_3_Location#
Bring Your Own Technology Standard	1.0	#4_4_Location#
Data Backup Standard	1.0	#7_2_Location#
Logging & Monitoring Standard	1.0	#5_3_Location#

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

Document	Version	Location
Disaster Recovery Standard	1.0	#6_2_Location#
Cryptography Standard	1.0	#7_4_Location#
Cloud Security Standard	1.0	#5_2_Location#
End User Protection Standard	1.0	#2_4_Location#
Network Security	1.0	#3_2_Location#
Third Party Risk Management Standard	1.0	#4_2_Location#
Acceptable Use Standard	1.0	#2_3_Location#
Employee Lifecycle Management Standard	1.0	#6_3_Location#
System Acquisition & Development Standard	1.0	#3_3_Location#
Security Incident Management Standard	1.0	#5_4_Location#
Change Management Standard	1.0	#3_4_Location#
Information Security Risk & Compliance Management Standard	1.0	#7_3_Location#
Physical Security Standard	1.0	#6_4_Location#

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.

Document	Version	Location
Personal Data Acquisition Standard	1.0	#2_1_Location#
Breach Notification Standard	1.0	#3_1_Location#
Personal Data Transfer Standard	1.0	#4_1_Location#
Personal Data Complaints Management Standard	1.0	#6_1_Location#
Personal Data Processing Standard	1.0	#7_1_Location#
Information Classification & Handling Standard	1.0	#5_1_Location#

7 Approval

Document SME:	#DPO#
Document approver:	#Author#
Review date:	#Effective_Date#

8 Version history

Version	Effective Date	Author	Change Notes
1.0	#Effective_Date#	#Author#	Initial Authoring

© Copyright material from the eu.uk.com GDPR Compliance Portal and Back Office. You may only use this information with a current membership. Unauthorized duplication or copying is prohibited by law.