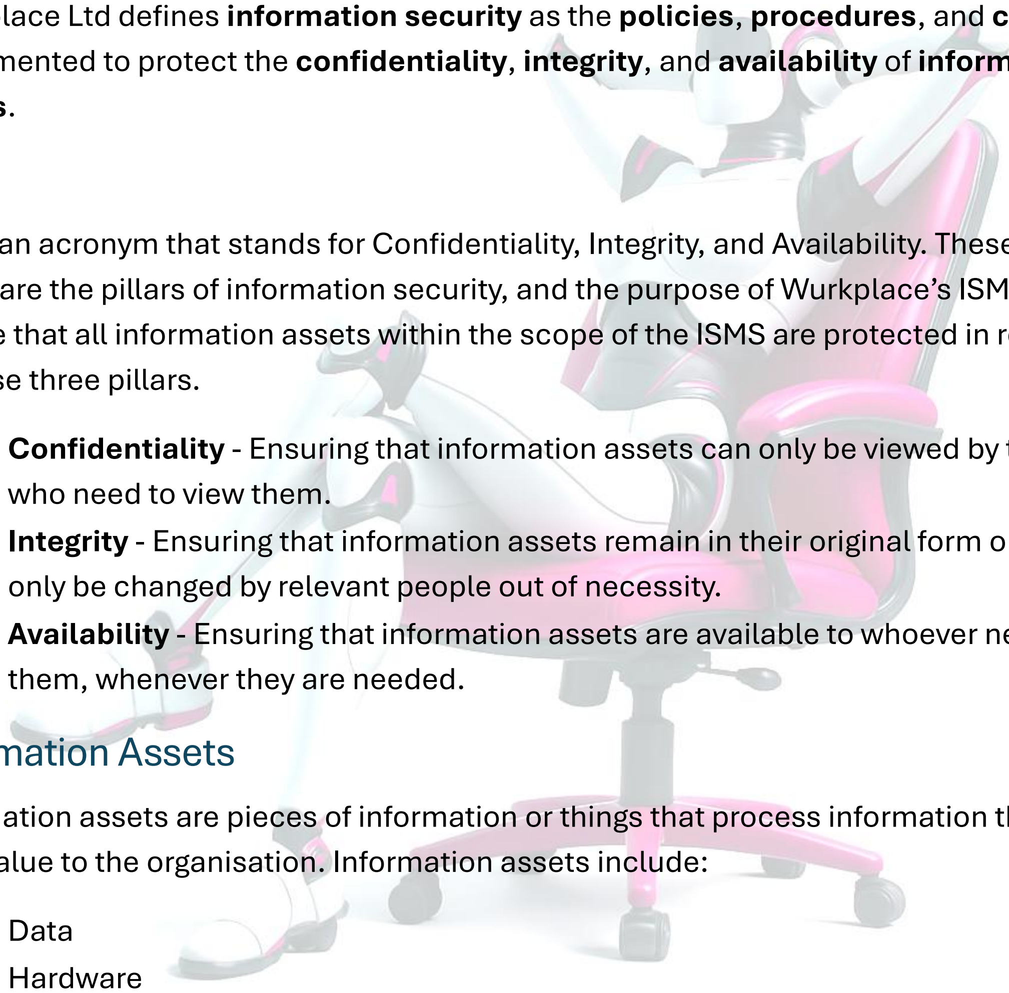
wurkplace hub

Empowering Business, Elevating Teams.

Information Security Policy

Note: This document is a simplified version of Wurkplace's Information Security Policy intended for transmission to external parties.



Definitions

Information Security

Wurkplace Ltd defines **information security** as the **policies**, **procedures**, and **controls** implemented to protect the **confidentiality**, **integrity**, and **availability** of **information assets**.

CIA

CIA is an acronym that stands for Confidentiality, Integrity, and Availability. These three terms are the pillars of information security, and the purpose of Wurkplace's ISMS is to ensure that all information assets within the scope of the ISMS are protected in respect of these three pillars.

- **Confidentiality** - Ensuring that information assets can only be viewed by those who need to view them.
- **Integrity** - Ensuring that information assets remain in their original form or can only be changed by relevant people out of necessity.
- **Availability** - Ensuring that information assets are available to whoever needs them, whenever they are needed.

Information Assets

Information assets are pieces of information or things that process information that hold value to the organisation. Information assets include:

- Data
- Hardware
- Software
- Services
- Locations
- People

ISMS

ISMS stands for Information Security Management System, and is the collection of policies, procedures, and controls within the ISMS' scope.

Policies, Procedures, and Controls

- Policies – High level statements of intent of the organisation regarding information security.
- Procedures – Formal instructions on completing specific information security tasks.
- Controls – Specific organisational, people, physical, or technological measures put in place to protect information assets.

Incident

An incident within the ISMS' scope refers to any circumstances where the CIA of information assets is affected.

Risk

A risk is a deviation from an expected outcome with a negative impact on objectives.

Control

A control is a measure put in place to mitigate or avoid the negative impact of a risk that occurs.

Non-conformity

A non-conformity is a failure to meet a mandatory requirement of the ISO 27001 standard.

Interested Parties

The people, groups, or organisations that either impact or are impacted by Wurkplace. These parties are defined in the Context of the Organisation document.

Scope

These measures apply to all people, devices, systems, processes, geographic locations, and cloud services (information assets) under the organisation's control.

Objectives

The ISMS addresses the following objectives:

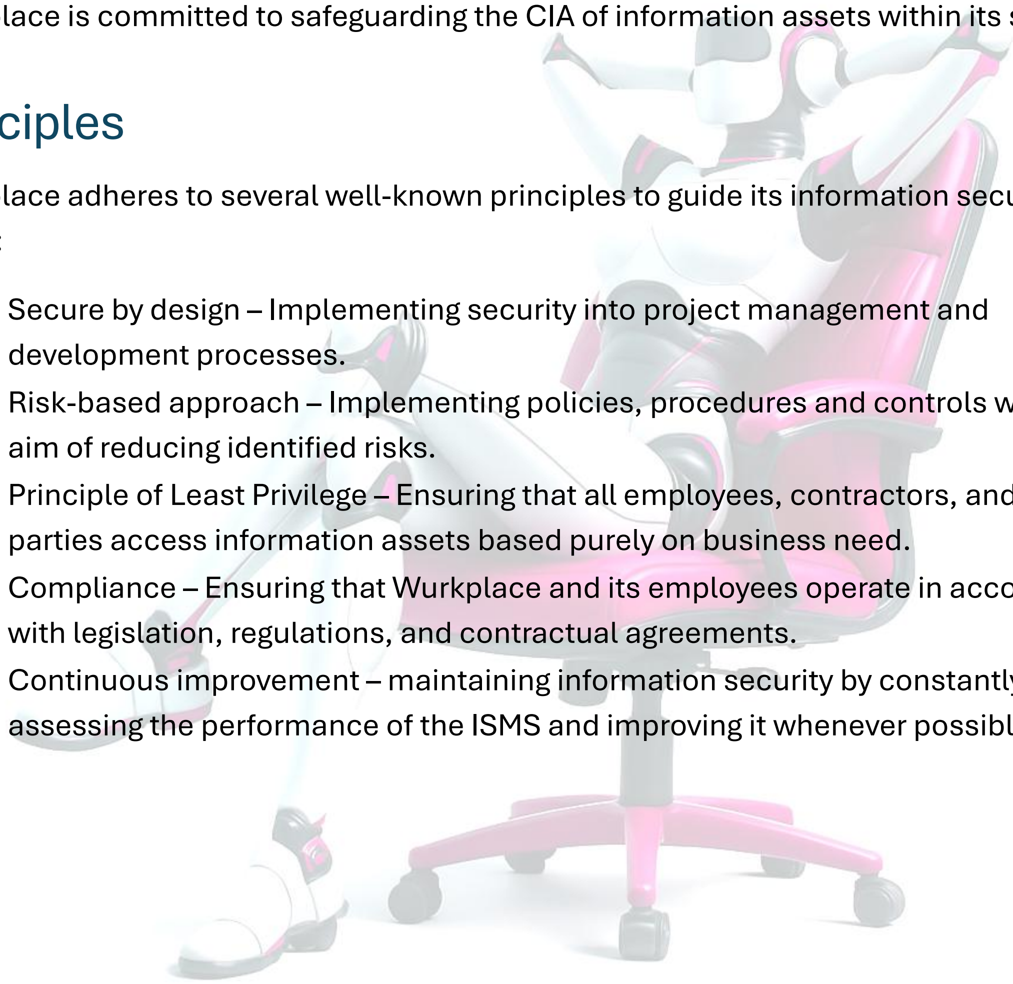
- The need to comply with regulation, legislation, and contractual agreements, including GDPR and Data Protection Act 2018
- Compliance with standards, including ISO 27001 and Cyber Essentials
- Build trust with clients and users
- Support business objectives

Wurkplace is committed to safeguarding the CIA of information assets within its scope.

Principles

Wurkplace adheres to several well-known principles to guide its information security policy:

- Secure by design – Implementing security into project management and development processes.
- Risk-based approach – Implementing policies, procedures and controls with the aim of reducing identified risks.
- Principle of Least Privilege – Ensuring that all employees, contractors, and third parties access information assets based purely on business need.
- Compliance – Ensuring that Wurkplace and its employees operate in accordance with legislation, regulations, and contractual agreements.
- Continuous improvement – maintaining information security by constantly assessing the performance of the ISMS and improving it whenever possible.



Policies

The ISMS contains topic specific policies, listed below:

- Acceptable use of Assets Policy
- Backup Policy
- Clear Desk and Clear Screen Policy
- Cloud Services Policy
- Cryptographic Controls Policy
- Data Retention Policy
- Firewall and Network Security Policy
- Incident Response Policy
- Information and Classification Handling Policy
- Information Transfer Policy
- Malware Protection Policy
- Mobile Devices and Teleworking Policy
- Password Policy
- Physical and Environmental Security Policy
- Privacy and Protection of Personally Identifiable Information Policy
- Secure Configuration Policy
- Secure Development Policy
- Secure Disposal Policy
- Supplier Relationships Policy
- Technical Vulnerability Management Policy
- User Access Control Policy

Roles and Responsibilities

Wurkplace assigns two responsibilities to the implementation and enforcement of its ISMS: Top Management, which oversees the ISMS and ensures it is supported, and the Information Security Officer, who is responsible for creating, implementing, monitoring, evaluating, and improving the ISMS.