# Security Directives

# Business objectives for security

These directives outline the overarching <company name> business goals for driving the need for robust security measures in our multi-cloud environment. These objectives provide the foundation for our security governance, ensuring that our approach is aligned with our broader business strategy and operational requirements.

**Protecting assets**

<company name> has valuable information assets. If these assets are shared inappropriately, their value could drop greatly. Sharing some assets wrongly could also seriously harm the company. If unauthorized changes are made to this information, it could affect the company's business operations. On the other hand, blocking legitimate access to these assets could cause significant problems. Ensure the confidentiality, integrity, and availability of critical business data and IT assets across all cloud platforms, mitigating risks related to data breaches, unauthorized access, and data loss.

**Regulatory Compliance**

Adhere to relevant industry standards and regulatory requirements, reducing legal and financial risks by ensuring compliance across multiple jurisdictions and regulatory frameworks.

**Business Continuity**

Maintain business operations in the face of security incidents and threats, ensuring minimal disruption to services and the ability to recover swiftly from any security breaches.

**Reputation and Trust**

Safeguard the organization's reputation by demonstrating a strong commitment to security, thereby enhancing trust with customers, partners, and stakeholders.

# Scope

These directives apply to all employees, contractors, part-time, and temporary workers, and anyone else working on company premises or with access to company information or systems.

**Cloud Environments**

This document applies to all cloud environments utilized by the organization, including public, private, and hybrid cloud models, across all service models (IaaS, PaaS, SaaS).

**Stakeholders**

Identifies all internal and external stakeholders involved in or affected by our multi-cloud security governance, including IT, security teams, cloud service providers, and end-users.
Employees, business partners, and contract personnel using any computer-related technology need to understand the rules and requirements of these directives.

**Data and Applications**

Covers all data and applications hosted in the cloud, including those in transit between cloud environments or between cloud and on-premises infrastructure.

# Security objectives

<company name> understands the importance of information and IT assets as key to the business. Every user is responsible for protecting these assets. <company name> has a thorough security policy and compliance program in place that:

* Addresses business risks
* Follows widely recognized information security standards
* Meets all relevant legal and regulatory obligations

# Principles

Information security is about managing risks to keep information safe, ensuring its confidentiality, integrity, and availability. We establish this through policies and standards that guide users and administrators on how to reduce risks while balancing the cost of these actions. Policies set the overall approach to information security, while standards provide detailed steps to achieve policy goals.

**Protection of assets**

<company name> is dedicated to protecting all information used by the company and held for employees, investors, partners, customers, and government agencies.

**Policies, standards and guidelines**

We create clear security policies, standards, guidelines, and procedures to outline security expectations and help in choosing and applying security measures.

**Risk management**

<company name> will manage risks carefully to reduce them or make sure they are within the company risk tolerance.

**Responsibility**

We make sure everyone understands their personal responsibility for following information security policies in their work.

**Awareness**

Through education and training, we make sure everyone knows about security risks and how to follow the company's security policies.

**Information classification**

We classify information by its importance to protect it properly, using the <company name> Information Classification Guide.

# Roles and responsibilities

Everyone working for the company, including employees, contractors, and temporary or part-time workers, must make sure they use company information correctly for business purposes only. They must prevent any misuse, changes, or threats to this information and not allow anyone unauthorized to access it.

The security management team is in charge of making sure the right security measures are in place across the company. A specific group within this team ensures that systems for logging in and getting access to information are up-to-date and correct. This team also decides how to put security rules into action and helps guide others in making good security policies. People who create and develop our software are responsible for incorporating these security rules effectively and managing them within their projects.

<company name>'s management has to regularly check all stored information, applications, and information systems to decide what security measures are needed based on how important the information is to the company, its value, and how much it might be worth to competitors. These checks should be documented and done at least once a year. The security team will also continuously assess risks to the company's information and systems.

Each department head must assign someone to be in charge of the information assets within their area, as directed by the security management team.

* Executive Management is in charge of overseeing information security and making sure that the company follows all security policies and practices.
* The Information Security Leader ensures the right security measures are in place and followed across the company. This person is also responsible for setting up security policies, advising on security matters, raising awareness about security, and overseeing security audits and teams.
* The Security Policy and Compliance Governance group, led by the Information Security Leader and including members from different parts of the company, supports and promotes security initiatives, reviews security policies, and defines security roles and responsibilities within the company.