Information Security Policy for Examplecorp ABC

Version: 2.0 **Date:** 2025-04-10 **Approved by:** Management Board

1. Vision and Strategic Commitment

Examplecorp ABC's vision is to [insert company's overall vision, e.g., "be the most innovative and trusted partner in our industry"]. Achieving this relies fundamentally on the trust of our clients, partners, and employees. Information security is not merely a technical function; it is a **strategic imperative** for building and maintaining this trust, protecting our brand reputation, and ensuring our long-term competitiveness and success.

We commit to:

- **Integrating information security** as a core component of all business processes and decisions.
- **Proactively identifying and managing risks** related to our information assets.
- **Ensuring the confidentiality, integrity, and availability** of all information we handle.
- **Meeting or exceeding** legal, regulatory, and contractual information security requirements.
- **Fostering a strong security culture** where every employee understands their role and actively contributes to information security.

Our long-term goal is for information security to be a **business enabler**, supporting innovation and efficiency whilst safeguarding our valuable assets.

2. Purpose and Scope

The purpose of this policy is to establish the framework and fundamental requirements for information security within Examplecorp ABC. It aims to provide both strategic direction and specific operational rules to protect the organisation's information assets.

This policy covers all information owned, processed, or stored by Examplecorp ABC, regardless of format or location. It applies to all employees, management, board members, contractors, temporary staff, and third-party suppliers who have access to company information or systems.

3. Fundamental Security Principles (Strategic Basis for Operational Rules)

All handling of information and systems within Examplecorp ABC shall be guided by the following principles:

- **Confidentiality:** Information must only be accessible to authorised individuals.
- **Integrity:** Information must be accurate, complete, and protected from unauthorised modification or deletion.
- **Availability:** Information and associated systems must be accessible to authorised users when needed.
- **Least Privilege:** Users shall only be granted the access necessary to perform their job functions.
- **Risk-Based Approach:** Security measures shall be based on assessed risks and proportionate to the value and sensitivity of the information.

- **Accountability:** All actions within systems should be traceable to a responsible individual or process.

4. Operational Guidelines and Responsibilities (Daily Work)

To achieve our strategic objectives and uphold these principles, the following is required from every employee in their daily work:

- **4.1 User Accounts and Passwords:**
    - Your user account is personal and must not be shared. You are responsible for all activities conducted under your account.
    - Use strong, unique passwords for all systems and change them according to company guidelines. Enable multi-factor authentication (MFA) where available. This is a basic measure to protect both your and the company's information (*Confidentiality*).
    - Lock your computer and mobile devices when leaving them unattended.
- **4.2 Email and Communication:**
    - Be critical of unexpected or suspicious emails, especially regarding links and attachments (phishing). Verify the sender's identity if uncertain. Mishandling can lead to breaches and damage the company's *reputation*.
    - Send sensitive or confidential information only via approved, secure channels (e.g., encrypted email).
- **4.3 Physical Security:**
    - Protect physical documents and storage media from unauthorised access. Keep sensitive materials locked away when not in use.
    - Be aware of your surroundings and report unfamiliar individuals or suspicious activities on company premises. Help maintain perimeter security.
- **4.4 Use of Equipment and Software:**
    - Use only equipment and software provided and approved by Examplecorp ABC for work purposes.
    - Installation of unauthorised software is prohibited as it can introduce vulnerabilities threatening *all* our security principles.
    - Keep systems and software updated according to IT department instructions.
- **4.5 Handling Information:**
    - Handle all company information (including client data, personnel data, trade secrets) with appropriate care, according to its classification and applicable legislation (e.g., GDPR). This is crucial for fulfilling our *strategic commitment* to trust and regulatory compliance.
    - Do not store or process company information on personal devices or unapproved cloud services without explicit authorisation.
    - Ensure proper deletion or destruction of information when it is no longer needed.

- **4.6 Remote Working:**
  - When working outside the office, ensure you use a secure network connection (e.g., VPN) and that your work environment protects information from unauthorised viewing. Flexibility must not compromise our *strategic commitment* to security.

5. Incident Management

All suspected or actual information security incidents (e.g., viruses, data breaches, lost equipment, suspected unauthorised access) must be reported immediately to the IT Helpdesk or your line manager, following the established procedure. Swift and accurate management is critical to minimise damage and ensure *business continuity*.

6. Training and Awareness

Examplecorp ABC views training and awareness as a **strategic investment** in our security posture. All employees are required to participate in mandatory security training and stay informed about current policies and procedures. An informed workforce is our most important line of defence.

7. Compliance and Consequences

Compliance with this policy is mandatory for everyone it covers. Violations may result in disciplinary action, including warnings, reassignment, or termination of employment/contract, as well as potential legal action. Non-compliance risks not only operational disruption but can severely damage the company's *strategic assets*, such as brand reputation and client trust.

8. Policy Review and Continuous Improvement

This policy shall be reviewed at least annually, or as needed, by the designated function (e.g., Information Security Committee or Head of IT) to ensure it remains current, relevant, and effectively supports the organisation's *strategic goals* while adapting to the evolving threat landscape. Suggestions for improvement are encouraged.

9. Contact Information

For questions about this policy or to report an incident, please contact:

- IT Helpdesk: [Phone Number], [Email Address]
- Information Security Manager: [Name], [Email Address]
- Your Line Manager