Operational Information Security Policy for Examplecorp ABC

Version: 1.0 **Date:** 2025-04-10 **Approved by:** Management Board

1. Introduction and Purpose (Strategic)

Information security is fundamental to Examplecorp ABC's operations and the trust placed in us. This policy **shall** guide all employees in their daily activities to protect the company's information assets. Every employee **must** understand and adhere to these guidelines. Good cybersecurity is **not** solely the responsibility of the IT department, but everyone's. The purpose of this policy is to provide clear operational guidance and ensure everyone understands the importance of protecting company information.

2. Scope

This policy applies to all employees, contractors, and temporary staff at Examplecorp ABC who have access to the company's information systems, network, and data.

3. Guidelines for Daily Work (Operational)

To maintain a good level of cybersecurity in daily work, the following applies:

- **3.1 Access and Passwords:**
  - Your password is personal. **Never** share your password with anyone else, either internally or externally.
  - Passwords **shall** be complex and changed regularly according to IT department recommendations.
  - You **should** use a password manager to handle your passwords securely.
  - Your computer screen **must** be locked when you leave your workstation, even for short periods, to prevent unauthorised access.
- **3.2 Email and Communication:**
  - Always be vigilant about phishing attempts and suspicious emails. Do **not** click on unknown links or open unexpected attachments.
  - Sensitive information **shall** only be sent via approved and encrypted channels.
  - You **need** to verify the sender's identity if you are uncertain, especially when requests seem unusual or urgent.
- **3.3 Physical Security:**
  - Do **not** leave sensitive documents visible on your desk when unattended. Store them securely.
  - Visitors **shall** always be signed in and wear a visible visitor badge. Be aware of unfamiliar individuals in company premises.
- **3.4 Use of Equipment and Software:**
  - Only use equipment (computers, mobiles, etc.) and software approved by Examplecorp ABC.

  - Installation of software that is **not** approved by the IT department is strictly **forbidden**.
  - Systems and software **must** be kept updated according to the IT department's instructions. Any suspected malicious activity on your computer **shall** be reported immediately.

4. Data Handling (Strategic & Operational Element)

All company data **shall** be handled according to current legislation (e.g., GDPR) and internal classification rules. Sensitive information must **not** be stored in unsecured locations like personal cloud services or unapproved USB drives. You **need** to ensure data is securely disposed of when no longer required.

5. Incident Reporting

All suspected or confirmed security incidents (e.g., suspected breaches, lost equipment, virus infections, phishing attempts) **must** be reported immediately to the IT helpdesk or your line manager, following the current incident management procedure. Prompt reporting is crucial to minimise potential damage.

6. Responsibilities and Compliance (Strategic)

Every employee is responsible for adhering to this policy. Managers **shall** ensure their teams are aware of and understand the policy. The IT department is responsible for technical controls and support. Non-compliance is **not** acceptable; breaches of this policy may lead to disciplinary action, up to and including dismissal, and potentially legal consequences.

7. Review and Updates

This policy **shall** be reviewed and, if necessary, updated at least annually, or more frequently if circumstances require (e.g., changes in the threat landscape or regulations).

8. Contact

For questions regarding this policy, please contact the IT Helpdesk or your line manager.