Probi Information Security Directive

Approved by the Management

This is a summary version of Probi's internal policy. This document only presents the main objectives of the policy.

The **Probi Information Security Directive** outlines guidelines to protect the confidentiality, integrity, and availability of Probi Group's data, including both digital and printed materials. Here is a one-page summary of its key points:

1. Purpose

The directive ensures a secure information environment by establishing security measures and promoting responsible behavior among employees, partners, and consultants to prevent unauthorized access, damage, or loss of Probi's information and equipment.

2. Scope

This directive applies to all entities within Probi Group and covers all IT systems, data, and equipment. Employees are responsible for ensuring their devices are secure, their information is protected, and they adhere to the security measures.

3. Key Security Measures

- **Identity & Accounts**: Employees must protect their usernames and passwords, use strong passwords, and avoid sharing credentials.
- **Devices**: Devices must be kept secure, and employees should avoid leaving them unattended or exposed in public spaces.
- **Information**: Employees must store data in approved locations (e.g., OneDrive), avoid storing information locally, and be vigilant about phishing and malware.
- **Clean Desk Policy**: Workspaces should be cleared of sensitive information, and devices must be locked when unattended.

4. Incident Reporting

Any security incidents, including theft, data breaches, or suspicious activity, must be reported immediately to the IT Servicedesk to minimize potential damage.

5. Email, Internet, and Social Media Use

- **Company Email**: Should be used only for business purposes, with caution to avoid phishing or unauthorized communication.
- **Internet Usage**: Should be limited to work-related activities, avoiding inappropriate sites or downloads.
- **Social Media**: Employees must maintain professional behavior on social media and avoid sharing Probi's confidential information.

6. Probi's Monitoring and Rights

Probi monitors the use of its IT systems for security purposes and may review electronic communications for compliance. Violations may result in penalties, including termination.

7. Responsibilities and Misuse

Employees are responsible for adhering to the directive. Misuse or non-compliance may lead to disciplinary actions, and employees must return all company property and information upon leaving the company.

This directive ensures that all employees contribute to maintaining a secure digital and physical environment for Probi's information.