SECURITY POLICY

THE SECURITY POLICY IS A PART OF THE PPHS CYBERSECURITY STANDARD FOR SMALL AND MEDIUM-SIZED ENTERPRISES AND PUBLIC INSTITUTION DEVELOPED BY THE POLISH PLATFORM FOR HOMELAND SECURITY.

TABLE OF CONTENTS

03

POLICIES, PROCEDURES AND INSTRUCTIONS

Policy is a formal, short and high-level statement or plan which defines the overall objectives of the organization as well as establishes important assumptions, values and commitments by which the company is governed and which should be followed by employees. In addition, it may contain references to procedures for particular subject areas which specify the policy or policies. However, instructions, which in turn can supplement the procedures are the most detailed.

In other words: policies define what should be protected and what are the basic principles and objectives. Procedures define how to protect resources or how to adopt policies. For example, in a policy, rules regarding passwords describe how passwords should be built, how they should be protected and how often they should be changed. A procedure for password management, on the other hand, would describe the process of creating new passwords, transmitting them, as well as ensuring the change of passwords on critical devices (however, there will not always be a one-to-one relationship between policies and procedures).

The main policy should be a public document, communicated to all stakeholders (employees and external parties). On the other hand, more detailed policies or instructions may be confidential documents, accessible only to specific audiences.

The policy should be a document approved by the company's management.

04

AN EXAMPLE OF A SIMPLE COMPANY'S SECURITY POLICY

Introduction

OBJECTIVE

The aim of the policy is to protect assets and ensure business continuity. It provides guidance to achieve these objectives. It has been prepared in accordance with the best practices and standards .... (i.e. PPHS Standard)

SCOPE

The principles of this Policy define the minimum requirements for ensuring a secure IT environment in the company. These principles apply to the company's management, employees, contractors, agents and suppliers. They also extend to the technology and equipment of the company's information resources.

COMPLIANCE

All Company employees are responsible for understanding and complying with all safety rules contained in this policy and accompanying documents. Non-compliance with the policy/breach of the policy may result in disciplinary action, including immediate release, criminal prosecution and/or loss of access to company's resources.

Any case of non-compliance must be reported.

05

COMPANY'S POLICY

Corporate information, facilities and all other assets will be used in an approved, ethical and lawful manner to avoid damage or loss of business continuity, adverse effects on financial interests or corporate image. The objective is also to comply with official, accepted usage policies and procedures. Staff will contact a chief information security officer (CISO) before taking any action that is not explicitly included in these policies.

ROLES AND RESPONSIBILITIES

The roles and responsibilities regarding acceptable use are defined in the following sections.

Chief Information Security Officer

The Chief Information Security Officer shall be responsible for establishing, adopting and updating the corporate security policy.

Board of Management

Managers (Board of Management) are responsible for:

- Informing staff of corporate policies on the acceptable use of information resources.
- Ensuring that staff under their supervision comply with these rules and procedures.

06

ROLES AND RESPONSIBILITIES

System administrators

Administrators are responsible for:

- Ensuring the availability, integrity and confidentiality of the systems and the data processed therein.
- Reporting suspicions or the occurrence of unauthorized activity.

All employees

All personnel will be responsible for:

- Compliance with official corporate policies on the acceptable use of information resources.
- Immediate reporting of suspicion or occurrence of any incidents.

Auditors

- Auditors are responsible for compliance control.

07

INFORMATION SECURITY POLICY

The organization must record, conserve and update its information resources (or assets) and provide adequate means to ensure the protection of the confidentiality, integrity and information availability owned by or entrusted to the company.

Information classification

All information, data and documents must be categorized and marked so that all users are aware of the ownership and classification of the information.

Storage and handling of information

All users of information systems must manage the creation, storage, transmission, correction, copying and deletion/disposal of data files in a way that protects the confidentiality, integrity and availability of such files.

Access control

Standards for controlling access to information systems must be established by the board of management and should take into account the need to balance constraints so that a balance is struck between the level of access restrictions and business needs. Access to resources should be limited only to the extent required by the business need.

08

PHYSICAL SAFETY

Appropriate safeguards for physical access to resources, commensurate with the level of acceptable risk identified, should be applied.

BUSINESS CONTINUITY

The continuity of important business processes is guaranteed through establishment of a formal and comprehensive business continuity plan.

SAFETY AWARENESS

An awareness program regarding information security should be implemented in order to increase the awareness of the company's employees and educate them about threats and appropriate security measures.

COMPLIANCE WITH SECURITY POLICY

Compliance with security policy is mandatory for all company's employees, contractors, agents and suppliers. Policy compliance must be enforced through periodic audits.

POLISH PLATFORM
FOR HOMELAND SECURITY

Polish Platform for Homeland Security

ul. Slowackiego 17/11
60-822 Poznań
www.ppbw.pl/en
tel.: +48 (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

European Funds Smart Growth

Republic of Poland

European Union
European Regional Development Fund

The project "Cybersecurity – PPHS Standard for SME and public institutions" was financed by the European Regional Development Fund.