Systembolaget Information Security Management - Pilot

This document is provided for informational purposes to current and prospective suppliers and contributors in the Pilot phase of the "PCF project". While the information can be shared within your organization, please contact Systembolaget for the most current version of this document when needed

INFORMATION MANAGEMENT, CYBERSECURITY, AND SECURITY REQUIREMENTS WORK

Information is one of Systembolaget's most valuable assets. Information assets refer to all information without exception, regardless of whether it is processed manually or automatically, and regardless of its form or the environment in which it occurs.

Systembolaget's intention with information security is to ensure efficient information supply and to avoid errors that affect the ability to conduct appropriate operations. The systematic security work aims to minimize risks and optimize opportunities. The work with IT and information security is systematic and long-term.

Systembolaget's information security work aims to ensure access to the right information for the right person at the right time and place through control and adequate protection. Information classification evaluates information based on the consequences of deficiencies in confidentiality, integrity, or availability and is divided into information protection classes. Protection needs and protective measures are based on ISK to minimize risks.

SYSTEMATIC DATA PROTECTION WORK

Systembolaget works in a structured and systematic manner with data protection issues throughout the organization. The starting point should always be to build in adequate protection in every processing of personal data and to have privacy-friendly settings as default settings. Systembolaget, as the data controller, takes full responsibility for the processing of employees', customers', suppliers', and other stakeholders' personal data.

All processing of personal data is permeated by the fundamental principles of data protection legislation, namely the principles of legality, transparency, accuracy, purpose limitation, data minimization, storage minimization, integrity and confidentiality, and accountability. In our routines, we incorporate the fundamental principles in a way that makes it easy to do the right thing. Below is an overview of how we work with the fundamental principles.

We protect the personal data we process and take appropriate security measures, both technical and organizational, to safeguard the data. We have clear instructions and routines for the organization on how personal data may be processed, and we have effective routines for reporting deviations and incidents. We provide clear instructions for personal data processing and follow up to ensure compliance with the instructions. We are aware of our processing activities and do not transfer or make personal data available outside the EU/EEA without first assessing the transfer and ensuring that the

personal data receives equivalent protection in the recipient country as within the EU/EEA.

We document and keep records of our personal data processing activities. We document our considerations and how we comply with the fundamental principles and data protection legislation.

Supporting the operational data protection work are Systembolaget's data protection ambassadors, Legal, and the data protection officer.

GOVERNING DOCUMENTS FOR SYSTEMBOLAGET'S IT DEVELOPMENT

Governing documents are a central part of IT development and ensure that the work is conducted uniformly, traceably, and in line with the organization's overall goals. They define principles, processes, and responsibilities for development efforts, and through the application of these, conditions for quality assurance, efficiency, and long-term management are created. The governing documents come from different levels, the levels that exist are:

- **External Environment**
  - Externally governing documents such as laws, regulations, and directives at the national and EU level
- **Policies**
  - For Systembolaget to act responsibly in all situations, it is required that all employees act in accordance with applicable laws, policies, internal rules, and our shared values. Systembolaget's policies are decided by the board once a year.
    - Systembolaget’s policies (in Swedish)
- **Internal Rules**
  - Employment
  - Digital Tools
  - Information Security
  - Systematic Data Protection
  - Ethical Governing Documents
  - Operations and Management
- **Internal IT Principles** for commercially managing the development, maintenance, and operation of IT delivery
- **Design Principles** in various areas
  - Cloud Principles, Cloud Governance, Integration Principles, Security Requirements, IT and Information Security Requirements, Risk Classification, and more

SYSTEMBOLAGETS IT AND INFORMATION SECURITY WORK

The company continuously works to enhance its ability to systematically manage IT and information security. In our security work, we follow MSB's framework for Information Security (ISO 27001) and CIS Controls V8. These frameworks contain a number of control points, some of which are outlined below.

Information Security and Data Protection

Systembolaget has processes and technical controls to identify and classify information based on sensitivity and value. The process aims to create a common increased understanding of the protective value of information based on Confidentiality, Integrity, and Availability so that we can adjust the security level of our solutions accordingly.

When handling personal data, an analysis is always performed on how the personal data will be processed (Privacy Impact Assessment) as well as an evaluation of whether there is a legal basis (Legitimate Interest Assessment) for processing the personal data.

Based on Information Classification and the need for data protection, our solutions are designed according to best practices. For solutions in our cloud infrastructure (MS Azure), we apply the MS Well Architected Framework and the security principles found there. The overarching guiding principles for our solutions are Zero Trust and Least Privilege Access for both users, devices, and systems.

Sensitive data is protected through encryption both at rest and during transmission.

Inventory and Control of Software

Systembolaget uses tools to automatically configure, distribute, inventory, and track all software installed on Systembolaget's network, including operating systems and applications. Devices are kept up to date with the latest security updates and patches to minimize vulnerabilities.

Account Management

Systembolaget assigns and manages permissions for user accounts centrally. The principle of least privilege is applied to ensure that users only have the permissions required for their tasks, and if users leave, their permissions are removed. Systembolaget's password policy ensures that all accounts are protected with strong authentication methods such as two-factor authentication.

Protection of Email and Browsers

Systembolaget uses email filtering services that provide protection from malicious attachments, harmful links, and phishing attempts (Advanced Threat Protection and behavior detection via EDR). Systembolaget's security measures to protect against browser-based threats include browser hardening, URL filtering, and safe browsing. Systembolaget's users are trained in secure email and browser practices to reduce the risk of social engineering and phishing attacks.

Protection Against Malware

Systembolaget uses antivirus and antimalware programs to detect and remove malware from systems and networks. EDR is implemented and monitored comprehensively.

Regular scanning is conducted on all systems to identify and remove malware. All antivirus and antimalware programs are continuously updated with the latest signatures and patches.

Security Operation Center SOC

Systembolaget uses a Security Operations Center (SOC) that provides round-the-clock monitoring and focuses on identifying security events and anomalies that may indicate threats. Any events are analyzed to assess whether they may develop into incidents. In the case of suspected or confirmed incidents, an initial analysis is conducted, after which the matter is handed over to a SecOps function for further handling.

The SOC function also works preventively by detecting potential threats at an early stage and by establishing and following relevant security policies. In addition, the SOC is responsible for ongoing reporting and compliance, which includes continuous external monitoring and internal reporting to ensure that the organization is aware of current threat landscapes and complies with applicable regulations.