Information Security and Data Privacy Policy

Background and purpose 1
Policy Statement 2
1. Information Security 2
2. Data Privacy 3
Audience 3
Roles and responsibilities 3
Exceptions 4
Monitoring of compliance 4
References 4

Background and purpose

The purpose of information security is to maintain a high credibility and service level towards shareholders, partners and customers. Credibility towards all stakeholders are achieved through ensure the availability and integrity of information and anticipate threats and minimize risks of information and information technology resources. This will ensure our business and financial performance.

The Information Security Policy and its supporting controls, processes and routines apply to all information used within MilDef Group, in all formats. This includes information processed by other organizations in their dealings with MilDef Group.

Policy Statement

Ensuring Availability – The ability of the infrastructure to function according to business expectations during its specified time of operation.

Information availability ensures that all stakeholders (shareholders, employees, customers, suppliers, and partners) can access information whenever they need it.

Maintaining Integrity – ensure the maintenance of, the assurance of, the accuracy and consistency of information over its entire life cycle. Meaning information cannot be modified in an unauthorized or undetected manner.

Maintaining Confidentiality – Ensuring information is not made available or disclosed to unauthorized individuals, entities, or processes.

1. Information Security

- Our information security risks shall be identified, managed and treated according to an agreed risk tolerance.
- Our authorized users shall be able to securely access and share information in order to perform their duties.
- Our physical, procedural and technical controls shall balance user experience and security.
- Our contractual and legal obligations relating to information security shall be met.
- Our business and administration shall consider information security in all processes.
- Individuals accessing our information shall be informed and educated of their information security responsibilities.
- Incidents affecting our information assets shall be resolved and learnt from to improve our controls.
- The company shall use relevant good practices and standards (i.e. ISO27000, CMMC etc.) to protect confidentiality, integrity and availability of information
- Corporate information assets shall be identified and classified to ensure that an appropriate level of security is applied.
- Business continuity planning shall be performed to ensure that serious disturbances and incidents can be managed efficiently. The plan shall be tested on a yearly basis.
- Premises and technical facilities shall be protected by appropriate physical security measures.
- In acquisition, development and maintenance processes, information security requirements shall be defined to ensure that an appropriate level of security is applied in systems, services and infrastructure during their whole life cycle.
- Risk analysis shall be performed recurrently to ensure a fit for purpose level of protection of the company’s information assets.

2. Data Privacy

To be able to operate, MilDef Group AB need to record, store, process, transmit, and otherwise handle personal information about individuals ("data subjects"). The company take these activities seriously and provides fair, secure, and fully legal management of private information. All activities related to processing of personal information are intended to be consistent with both generally accepted privacy ethics, standard business practices, local and regulatory laws, including the General Data Protection Regulation ("GDPR"). Personal information shall only be processed in line with these principles:

- **Lawfulness, fairness and transparency**, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- **Purpose limitation**, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **Data minimization**, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Storage limitation**, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- **Integrity and confidentiality**, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

Further, MilDef Group AB shall ensure that:

- Processes are implemented and necessary documentation is in place and kept updated to secure the data subject's rights
- Personal information processed within MilDef Group AB is protected in relation to its sensitivity
- Data protection agreements are signed with all third parties processing personal data on behalf of MilDef Group AB

It is the responsibility of all employees to ensure that the personal information to which they have access is treated accordingly with the six principles mentioned above.

Audience

The Information Security Policy and its supporting controls, processes and routines apply to all individuals who have access to MilDef Group information and technologies, including external parties that provide information processing services to MilDef Group.

Roles and responsibilities

The Director of IT is the owner of this policy.
Every manager is responsible for communicating this policy to their employees.
Every employee is responsible for acting in accordance with this governing document

Exceptions

There are no exceptions to this policy. Any need of exceptions to this policy must be clearly defined and documented. All exceptions shall be approved by the Board of Directors.

Monitoring of compliance

The policy is approved by Board of Directors. The policy is reviewed annually and revised if needed.
All employees are required to understand and comply with this Policy, violations may result in disciplinary actions including termination of employment.

References

Personal Data Routine
MilDef Information Security Management System