Pointsharp Information Security Policy

Classification:	Public
Publication No.:	PSE-IS21-01
Document version:	1.0
Document status:	Final
Date:	01 Jan 2023

Table of Contents

1 Purpose and definitions

The information assets that Pointsharp manages – both for itself, for its customers, and other parties – are of fundamental importance to Pointsharp's operations. The correct handling of these is important for the trust of employees, customers, partners, suppliers, and third parties. Information assets are all information that is of value to Pointsharp and the aforementioned parties, whether processed by analog or digital, automatically or manually and regardless of the form or environment in which it exists. The purpose of this information security policy is to demonstrate the management's intention to treat these assets by set goals and principles.

A systematic information security work is also the basis for well-functioning data protection work.

Information security can be summarized by the following requirements:

- **Confidentiality**, that information is not made available or forwarded to unauthorized persons in violation of legal requirements, rules, guidelines, or agreements.
- **Integrity**, that information is protected against unwanted change or deletion, whether intentional or unintentional.
- **Availability**, that information is available to the expected extent, for authorized users and within the desired time.
- **Traceability**, that all relevant actions associated with an individual's behavior can be saved and followed up over time.

2 Objectives and principles

By adopting this policy, Pointsharp undertakes to comply with the applicable information security requirements. The policy covers the entire operations of Pointsharp and contains objectives and principles so that:

- competence exists, and is constantly being developed, on how information security is ensured, maintained, and continually developed and improved;
- all relevant information assets are classified and handled according to established methodology;
- threats to information assets and services are continuously assessed and managed following a defined risk management process;
- the crisis management ability is continuously analyzed and maintained;
- unexpected and unwanted events leading to negative consequences are prevented;
- information security work is a natural and integrated part of the business;
- Information Security Management System (ISMS) and associated security measures are periodically audited to achieve continuous improvement; and
- discovered incidents, threats, and risks are reported for further processing.

3 Responsibilities

Responsibility for Pointsharp's information security work must comply with normal delegated operational responsibility at all levels.

The **Board** expresses its goals and principles by establishing Pointsharp's Information Security Policy.

The **Management Team**, led by the **CEO**, has the ultimate responsibility for Pointsharp's information security work and approves and adopts information security regulations. The Management Team owns and is responsible for Pointsharp's infrastructure, services, systems, and applications and appoints information and system owners for these.

The **Strategic Security Team** works strategically with the goals for the information security work at Pointsharp, the governing policies, and how the information security work is to be organized. The team is responsible for the overall risk management of Pointsharp's operations and makes follow-ups on the information security goals. The team works operationally with information security issues that may significantly affect Pointsharp's operations as a whole.

The **Operational Security Team** works operationally and to some extent strategically with risk and incident management, processes, instructions, and other aspects of the practical security work within Pointsharp.

The **Security Manager** has the overall responsibility to coordinate the systematic information security work so that the business complies with laws and regulations regarding confidentiality, integrity, availability, and traceability. The Security Manager leads the work of the two Security Teams (Strategic and Operational) and reports directly to the Management Team. The Security Manager creates information security training for all internal and external employees with the goal to keep everyone up to date with new and updated regulations as well as new threats and risks.

The **IT Security Manager** has the overall responsibility to coordinate the IT security work within Pointsharp and to interpret the IT solutions necessary to uphold what is stated in information security policies, guidelines, and instructions. The IT Security Manager supports the Pointsharp organization with evaluations concerning IT security for new systems and services as well as at changes in current systems and services. The IT Security Manager works closely with the IT department on practical IT implementation and to plan the roadmap for implementations.

The **Incident Manager** works operationally to bring risk and incident processes forward.

Each department owns and is responsible for its business-specific infrastructure, services, systems, applications, and information assets and appoints owners for these.

All employees (internal and external staff) have a responsibility to maintain information security, report information security incidents, and to participate in annual training.

Managers and **Assignment Managers** are responsible for ensuring that all employees undergo initial and annual information security training.

The **Internal Auditor** works on behalf of the Board and reports to the Management Team.

4 Deviations and exceptions

In the event of deviations or exceptions from this policy or related regulations, these shall be reported to the Incident Manager, Security Manager, or another member of the Operational Security Team. The Incident Manager is responsible for assessing the severity of an incident in consultation with the Operational Security Team and together deciding on appropriate measures.

More serious incidents and events that may harm Pointsharp must be reported to the Management Team as soon as possible to minimize damage and prevent similar incidents. In cases where exceptions need to be made from decided and applied regulations, a risk analysis shall be carried out and proposals for exceptions shall be presented to the Operational Security Team for further decisions. Accepted exceptions (with compensating measures) can only be valid for 12 months.

5 Review and follow-up

The Information Security Policy, and the related regulatory frameworks for information security, must be reviewed and updated at least once every 12 months or if significant changes in the organization or the outside world occur. This is to ensure the continued suitability, accuracy, and effectiveness of the policy. The review will include an assessment of Pointsharp's possibilities to improve its regulatory framework and the organization's approach to information security based on changes in Pointsharp's environment, business conditions, legal requirements, and technical environment. The annual review shall be done so that the entire business is reviewed every 3 years.

6 Related documentation

The Information Security Policy describes Pointsharp's intentions regarding information security. To meet the needs of the business, there are additional and more detailed instructions and guidelines regarding what has to be implemented, and in what way, for the policy to be complied with.

7 Validity of the Information Security Policy

The Information Security Policy is reviewed and approved by the Pointsharp Board in December each year and is valid from January 1st. An audit log is updated with a new decision date and a description of any changes.

8 Document history

Version	Date	Author	Change description
1.0	2022-12-21	Stefan Jacobsson	Reviewed and approved with no changes.

Version	Date	Author	Change description
1.0	2021-12-22	Stefan Jacobsson	First version of Pointsharp's information security policy.

POINTSHARP

Website
https://www.pointsharp.com

Copyright

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification:	Public
Publ. No.:	PSE-IS21-01
Document version:	1.0
Document status:	Final
OID:	
Published:	01 Jan 2023