Information Security Policy

231101

POLICY

Established by the Director General on: 17 October 2023
Enters into force on: 1 November 2023
Ceases to apply on: 1 November 2026

Person responsible: Security Office
Ref. no.: A2023/2860

Information security policy

Statistics Sweden’s activities - from questionnaires sent to enterprises and individuals to the final publication of survey results on the agency website or their delivery as part of commissioned services - involve extensive data handling. Furthermore, Statistics Sweden’s collaboration with other Swedish and foreign authorities and organisations requires sound information security.

Therefore, it is essential that information security issues are handled prudently and methodically. The data used and processed by Statistics Sweden constitutes an important strategic asset that must be protected.

Information is defined as all types of data used in the operations, regardless of whether the data is oral or written, and regardless of how it is processed, stored or transported.

General requirements

- Most security efforts are to be carried out at department and unit level, i.e. with those who most closely handle the information.
- The security work must be carried out systematically and be based on the agency's regulations for information security
- All information and all information systems must have clear ownership and designated responsibility within the agency.
- Information security is to be integrated into administration activities, projects and development and be included as a natural part of the daily work.
- All personnel is to be familiar with and apply current guidelines on information security. The immediate manager must provide support and guidance in this.
- All personnel must be regularly trained in security.
- Expectations, training and requirements regarding information security apply to both own employees as well as companies and personnel hired for special assignments.
- Requirements and follow-up of security must take place in procurements and other external cooperation.

- The assignment and removal of access control is to follow established guidelines. Users may only have the authorisations required for their working duties.
- All personnel are to be informed that their activities in the information systems may be monitored and reviewed.
- Information security activities are to apply a risk-based approach.
- Risk and vulnerability analyzes must be carried out within the agency, after which the necessary measures must be taken to ensure that information has the right protection.
- A continuity plan is to be in place in the event of particular events and crisis situations.
- Procedures for handling security incidents are to be in place.
- Compliance with guidelines is to be checked through regular reviews and controls.

Statistics Sweden's information security management system (SCB LIS)

Information security operations at the agency are to be governed by requirements contained in Statistics Sweden's information security management system (SCB LIS). SCB LIS is managed by the Security Office at Statistics Sweden. These must be regularly followed up and updated if necessary.

SCB LIS comprises the following documents:

- Information security policy
- Guidelines
- Instructions
- Training material
- Check lists, and
- Templates.