Policy

Information Security Policy for DIFO and Punktum dk

Group	Security Policy
Approved by	Jakob Bring Truelsen
Approved	06.06.2025
Responsible	Erwin Lansing
Version/ID	24.0.0 / 00002
Edited by	Jakob Bring Truelsen
Edited	06.06.2025
Review date	25.06.2025
Document	Final
Security classification	Public information
Information type	Information – if no content
Type	Security Policy

Information security policy for DIFO and Punktum dk

About the policy

This policy applies to both DIFO and Punktum dk.

Since Punktum dk is the operating company, Punktum dk is referred to below as the central unit, despite the fact that the policy applies to both DIFO and Punktum dk.

The policy has been continuously expanded and revised. The latest in June 2025.

Information security policy for Punktum dk

This policy is Punktum dk's overall framework for information security.
The information security policy, together with an ongoing risk assessment, creates the basis for taking measures that effectively and adapted to our circumstances ensure that critical and sensitive information and information systems maintain their confidentiality, integrity, authenticity and availability.

- Confidentiality, which is to ensure that information is protected against disclosure and unauthorized use, as well as any other requirements imposed by authorities, customers, DIFO and Punktum dk's management.
- Integrity, which is to ensure that information is complete, accurate and reproducible, and that IT programs used function correctly.
- Authenticity, which is to ensure that information is genuine and that there can be confidence in the validity of a transmission, a message or sender.
- Availability, which is to ensure that information with associated programs and facilities are available at the agreed times.

The information security policy must support the expectations and perception of DIFO and Punktum dk in the environment as a trustworthy and respected company and administrator of domain names and contribute to creating a security culture.

Objective

Punktum dk wants to maintain and continuously expand an information security level that meets the requirements of ISO 27001, Information Security Management Systems (ISMS). The requirements are tightened in well-defined areas where there are special legal requirements, contractual conditions or special risks identified in the annual risk assessment.

Punktum dk is covered by NIS and will also be covered by NIS2, because we are part of critical Danish infrastructure. NIS has been able to be handled within the framework of ISO 27001. NIS 2 is expected

to give rise to adjustments. The adjustments are currently being implemented in both systems and procedures.

Punktum dk uses incident reporting and handling to improve the processor. In addition, NIS2 will strengthen and streamline the incident process.

It is Punktum dk's goal to ensure:

That Punktum dk, by virtue of efficient, modern and secure data processing, has the best conditions to continuously optimize the administration of domain names without compromising data security and operational stability, while at the same time appearing as a trustworthy and respected company, partner and employer.

This must be done, among other things, by complying with ISO 27001, Information Security Management Systems (ISMS), including

- ensure that data and information are correct, accessible and used correctly by persons who are legally required to use them,
- prevent accidents and damage that may occur and limit the consequences of any accidents and damage to an acceptable level for Punktum dk (and the outside world),
- ensure that the continuation of Punktum dk's information systems after breakdowns and/or damage can be done within an acceptable time frame,
- ensure access control so that unauthorized persons cannot immediately gain access to data and systems that can be misused to the detriment of Punktum dk, our customers, employees and business partners,
- establish appropriate assurance that attempts to violate or disregard the security measures will be discovered to the greatest extent possible, and that the activity can be traced back to the person(s) who may be involved,
- ensure that employees achieve and maintain the necessary security awareness,
- ensure that employees are assured of security so that there is no incentive to hide any mistakes that may have been made, ensure that Punktum dk complies with legislation, regulations and agreements entered into agreements,
- ensure that cross-organizational contingency management is necessary for the continued operation of Punktum dk. ensure that information security is continuously adapted and improved to changing environments and new threats.

The above goals are specified in a number of measurement points, which are continuously updated and form the basis for decisions on adjustments or new initiatives to promote information security.

Scope

The information security policy applies to all our employees and others who are authorized to use

Punktum dk's IT assets. These include all information systems (machines, programs, communication systems) used by Punktum dk, regardless of whether they are stationary, portable, used at partners' addresses, in private homes via a network or as stand-alone.

Relevant requirements for compliance with the information security policy are incorporated into cooperation agreements with external suppliers, partners, service organizations, landlords, etc.

Management ensures that the information security policy is reassessed and updated when special circumstances warrant it, but always at least once a year.

Organization and responsibility

The overall responsibility for information security in Punktum dk lies with the board of directors. The board of directors has delegated operational responsibility for the day-to-day operations to the executive board.

The executive board is responsible for determining the necessary security level and recommending major necessary activities for approval. In addition, the executive board must ensure that all employees, suppliers, partners and consultants working on behalf of Punktum dk comply with the requirements of ISO 27001 or equivalent information security standard and comply with this information security policy.

The security forum consists of the director, the information security officer, the security manager and the IT manager and is responsible for escalating preparedness and clarifying special incidents of an information security nature.

The IT manager and the security manager are responsible for continuously informing the executive board of special information security matters.

The executive board is informed by the executive board or by the chairman of the security panel if particularly critical information security matters arise.

Particularly critical information security matters are when the company cannot maintain the operation of administrative systems or the zone.

The Security Manager is responsible for coordinating all security work, including establishing, maintaining and coordinating the work in the organization.

To ensure the organization's compliance with legislation and its own rules, a compliance unit has been established to oversee this. The compliance unit includes the Security Manager, personnel from Operations and the legal department.

All Punktum dk employees are personally responsible for complying with and acting in accordance with the information security policy and following the guidelines and procedures that have been established.

Security awareness

With this information security policy, Punktum dk wishes to indicate that information security is a high priority. This is done by attention from management and by a clear allocation of security responsibilities.

All employees will be continuously informed and trained in information security to the relevant extent, so

that they are aware of security risks and able to follow the letter and spirit of the given policies and guidelines.

There is ongoing work to create knowledge about what constitutes good behavior within information security, and this is also continuously tested using external actors.

Exemptions

Only the management board can grant exemptions from the information security policy in specific situations. The security manager must be consulted prior to an exemption. The security manager will discuss the consequences of an exemption with the organization. The board of directors must be informed of significant exemptions.

The management board shall inform the board of exemptions that affect the operation of the company's administrative systems and the zone.

Information security breach

Punktum dk cannot accept breaches of information security that are due to intent or gross negligence. The management handles any sanctions in connection with intentional violations of the information security policy in accordance with applicable rules and procedures in Punktum dk.

A breach of information security that is due to intent will be corrected immediately, analyzed and prosecuted in accordance with applicable rules and procedures in Punktum dk.

References

This information security policy is elaborated with detailed implementation guidelines, including not least guidelines regarding general passwords and root passwords, in accordance with ISO 27001 and is further described in Punktum dk's employee handbook.

Approval

The information security policy is approved by the DIFO and Punktum dk board of directors and is reviewed at least once a year.

This information security policy was last approved by the board of directors on June 20, 2024 and is recommended to the board of directors for renewed approval in June 2025.