Policy

Information security policy for DIFO and Punktum dk

Group	Security policy
Approved by	Jakob Bring Truelsen
Approved	25.06.2026
Responsible	Erwin Lansing
Version / ID	24. 1.0 / 00002
Modified by	Erwin Lansing
Modified	24.06.2026
Next review date	24.06.2027
Document classification	Finally **Security** Public information **Type** Security policy
Review dato	24.06.2026

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 stated in the following as the central unit, notwithstanding that the policy applies to both DIFO and Punktum dk.

The policy has been continuously expanded and revised. No later than June 2026.

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 measures to be taken that effectively and in accordance with our circumstances ensure that critical and sensitive information and information systems retain their confidentiality, integrity, authenticity and accessibility.

- *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 the IT applications used function properly.
- *Authenticity*, which is intended to ensure that information is genuine and that the validity of a transmission, message or sender can be trusted.
- *Accessibility*, which is to ensure that information with associated programs and facilities is available at the agreed times.

The information security policy is intended to support the expectations and perception of DIFO and Punktum dk as a trustworthy and respected company and administrator of domain names, and to contribute to the creation of a security culture.

Objective

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

Punktum dk

Responsible	Erwin Lansing	**Version / ID**	24.1.0 / 00002	**Modified by**	Erwin Lansing
Modified	24.06.2026	**Next review...**	24.06.2027	**Document**	Finally
The safety cl...	Public information	**Type**	Security policy	**Review dato**	24.06.2026

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 and 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 course of events.

It is Punktum dk's goal to ensure:

That Punktum dk, by virtue of efficient, up-to-date and secure data processing, has the best prerequisites for continuously optimizing the administration of domain names without compromising on data security and operational stability, and 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, Management Systems for Information Security (ISMS), including

- ensure that data and information are accurate, accessible and used correctly by persons who should be able to lawfully use them;
- prevent accidents and damage that may occur and limit the consequences of any accidents and damages to a size acceptable to Punktum dk (and the outside world),
- ensure that the continuation of Punktum dk's information systems after breakdowns and/or damages can take place within an acceptable time frame,
- ensure access management so that unauthorised 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 safeguards that attempts to breach or disregard security measures will be detected to the fullest extent possible and that the activity can be traced back to the person(s) involved;
- ensure that employees achieve and maintain the necessary security awareness;
- ensure that employees are ensured security, so that there is no incentive to hide any mistakes made,
- ensure that Punktum dk complies with legislation, regulations and agreements entered into,
- ensure that cross-organisational contingency management is necessary for Punktum dk's continued operation.
- ensure that information security is continuously adapted and improved to changing surroundings 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 adaptations or new initiatives to promote information security.

Scope

The information security policy applies to all our employees and others who are approved 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,

Group	Security policy	**Approved by**	Jakob Bring Truelsen	**Approved**	25.06.2026
Responsible	Erwin Lansing	**Version / ID**	24.1.0 / 00002	**Modified by**	Erwin Lansing
Modified	24.06.2026	**Next review...**	24.06.2027	**Document**	Finally
The safety cl...	Public information	**Type**	Security policy	**Review dato**	24.06.2026

at partners' addresses, in private homes via networks or as stand-alone.

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

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

Organisation and responsibility

The overall responsibility for information security in Punktum dk rests with the Board of Directors. The Board of Directors has delegated operational responsibility to the Executive Board on a day-to-day basis.

The Executive Board is responsible for determining the necessary level of safety and recommending major necessary activities for approval. In addition, the Executive Board must ensure that all employees, suppliers, business 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 Board of Directors is informed by the Executive Board or by the Chairman of the Security Panel if particularly critical information security issues arise.

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

The Head of Security is responsible for coordinating all safety work, including establishing, maintaining and coordinating the work in the organisation.

To ensure the organization's compliance with legislation and its own rules, a compliance unit has been established to monitor this. The compliance unit includes the Head of Security, staff from Operations and from the Legal Department.

All Punktum dk's 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 paying attention on the part of the management and by a clear location of the

safety responsibilities.

All employees will be continuously informed and trained about information security to the appropriate extent, so that they are aware of security risks and able to follow the word and spirit of the given policies and guidelines.

We are continuously working to create knowledge about what constitutes good behaviour in information security, and this is continuously tested by the use of external actors.

Exemptions

Only the Executive Board can grant exemptions from the information security policy in specific situations. The head of security must be consulted prior to a waiver. The head of security uncovers the consequences of an exemption with the organization. The board must be informed of significant exemptions.

The Executive Board shall inform the Board of Directors 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 due to intentional or gross negligence. The Executive Board handles any sanctions in connection with intentional breaches of the information security policy in accordance with applicable rules and procedures in Punktum dk.

A breach of information security due to insanity will be corrected immediately, analyzed and reprimanded in accordance with applicable rules and procedures in Punktum dk.

References

This information security policy has been 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 DIFO and Punktum dk's Board of Directors and is reassessed at least once a year.

This information security policy was last approved by the Board of Directors on 17 June 2026 and will be recommended to the Board of Directors for re-approval in June 2027.