Information Security Policy for

DIFO and Punktum dk

Group Security policy
Approved by Jakob Bring Truelsen

Approved	22 June 2023
Responsible	Erwin Lansing
Version / ID	21.1.0 / 00002
Changed by	Erwin Lansing
Changed	22 June 2023
Review date	21 June 2024
Document	Final
Security classification	Publicly available information

Information Security Policy for DIFO and Punktum dk

About this policy

This policy applies to both DIFO and Punktum dk.

As Punktum dk is the operational company, Punktum dk is hereinafter referred to as the central unit, regardless of the fact that the policy applies to both DIFO and Punktum dk.

The policy has been continuously expanded and revised. Last in June 2023.

Information Security Policy for DIFO and Punktum dk

With this information security policy, which provides the general framework for information security at DIFO and Punktum dk, DIFO and Punktum dk wish to signal that information security is high on our list of priorities.

Together with continual risk assessments, the information security policy creates the basis for measures which ensure that critical and sensitive information and information systems maintain their confidentiality, integrity and availability, both effectively and in line with our circumstances.

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

The aim of the information security policy is to support the public's expectations and perception of DIFO and Punktum dk as a credible and respected company and administrator of domain names, that creates a security culture.

Objective

DIFO and Punktum dk wish to maintain and continually develop a level of information security that meets the requirements of ISO 27001, Information Security Management Systems (ISMS). The requirements are stricter in well-defined areas in which there are special legal and regulatory requirements, contractual issues or specific risks identified during the annual risk assessment.
Punktum dk is covered by NIS and will also be so by NIS2 since we are part of critical Danish infrastructure. NIS compliance has been achieved within the framework of ISO 27001. NIS2 is expected to give rise to adjustments.

Punktum dk uses incident reporting and handling to improve processes. In addition, NIS2 will strengthen and streamline the sequence of events.

DIFO and Punktum dk aim to ensure that:

That Punktum dk by virtue of an efficient, contemporary and secure data processing has the best prerequisites for continuously optimizing the administration of domain names without need for compromise on data security and operational stability while at the same time being perceived as a credible and respected company, partner and employer.

One way of ensuring this is to comply with ISO 27001, Information Security Management Systems (ISMS). This includes:

- Ensuring that data and information are correct, available and correctly used by individuals with the right to use them.
- Preventing accidents and damage that may arise and restricting the consequences of any accidents and damage to a level that is acceptable to DIFO and Punktum dk (and the public).
- Ensuring that DIFO and Punktum dk's information systems can resume operations after critical failure and/or damage within an acceptable time frame.
- Ensuring access control to prevent unauthorised persons from gaining access to data and systems that may be misused to the detriment of DIFO and Punktum dk and our customers, employees and partners.
- Establishing suitable safeguards to ensure that attempts to breach or override security measures will be detected to the greatest possible extent, and that the activity can be traced back to the individual(s) involved.
- Ensuring that employees achieve and maintain a necessary level of security- awareness.
- Ensuring that employees feel sufficiently secure in order to prevent any incentive to conceal any errors made.
- Ensuring that DIFO and Punktum dk comply with legislation, regulations and concluded agreements.
- Ensuring the establishment of a cross-organisational emergency management system, which is necessary for DIFO and Punktum dk's continued operations.
- Ensuring that information security is continually improved and adapted to changes in surroundings and new threats.

The above aims are specified in a number of reference points which are continually updated and form a basis for decisions on adjustments or new initiatives to promote information security.

Scope

The information security policy applies to all of our staff and anyone else authorized to us DIFO and Punktum dk's IT assets. These include all information systems (devices, programs, communications systems) used by DIFO and Punktum dk, whether they be stationary or portable, used at a partner's address, in private homes, via networks or stand- alone. Relevant requirements for complying with the information security policy are incorporated into cooperation agreements with external suppliers, partners, service organisations, our landlords, etc.

The management ensures that the information security policy is revised and updated where special circumstances so require, but at least once a year.

Organisation and responsibility

The board of directors has the overall responsibility for information security at DIFO and Punktum dk.

The executive board is responsible for defining the required security level and submitting for approval any major, necessary activities. Furthermore, the management shall ensure that all staff, suppliers, partners and consultants, who work on behalf of DIFO and Punktum dk, observe the requirements of ISO 27001, or equivalent information security standards, and comply with this information security policy.

The Information Security Committee consists of the CEO, the Information Security Manager and the Head of IT and is responsible for escalating emergency management and handling specific information security incidents.

The Head of IT and the Security Manager are responsible for continuously informing the management team of special information security issues.

The Information Security Manager is responsible for coordinating all security activities, including establishment, maintenance, and coordination of the work of the security organization.

To ensure the organization's compliance with legislation and its own terms, a compliance unit has been established, who oversees this. The compliance unit includes the Security Manager, personnel from the Operations and Legal departments.

All staff at DIFO and Punktum dk are personally responsible for complying with and acting according to the information security policy and adhering to the guidelines and procedures, that are established.

Security awareness

With this information security policy, DIFO and Punktum dk wish to signal that information security is high on our list of priorities. This entails vigilance on the part of management and a clear distribution of security-related responsibilities.

To the extent required, all employees will be regularly informed about, and trained in, information security, such that they are aware of security risks and able to comply with the wording and spirit of the given policies and guidelines.

There are ongoing activities to create knowledge about what is good behavior in the field of information security, just as this is continuously tested using external parties.

Dispensations

The executive board alone is entitled to grant an exemption from the information security. The Head of Security must be consulted prior to a dispensation. The Head of Security analyses the consequences of a dispensation with the organization. The board of directors must be notified of any significant dispensations.

Breach of information security

DIFO and Punktum dk cannot accept any breach of information security due to deliberate or gross negligence. The executive board deals with any sanctions in connection with deliberate violations of the information security policy, according to DIFO and Punktum dk's procedures and rules in force from time to time.

Any unintentional breach of information security will immediately be rectified and analysed and a verbal warning given according to Punktum dk's procedures and rules in force from time to time.

References

There are further details about this information security policy in DIFO and Punktum dk's employee manual, including detailed implementation guidelines and, not least, guidelines regarding general passwords and root passwords, in compliance with ISO 27001.

Approval

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

This information security policy was last approved by the board of directors on 22 June 2023 and proposed for renewal on 21 June 2024.