regionernes sundheds-it

Joint Regional Information Security Policy

Content

1. Objective 1
2. Organisation 3
3. Area of Validity 3
4. Targets 4
5. Approval 4

1. Objective

The Joint Regional Information Security Policy has been prepared in cooperation between the Capital Region of Denmark, Region Zealand, The Region of Southern Denmark, The Central Denmark Region, and The North Denmark Region.

Information security is fundamentally about the protection of information so that confidentiality, integrity and accessibility are maintained.

Every day sensitive personal data and other types of confidential information are processed by employees in the five Regions. It is imperative that data is correct, complete and accessible, as access to relevant, real-time personal data is a condition for good and cohesive treatment of the individual citizens. It is necessary to enable the Regions to continue to provide an up-to-date and efficient health sector.

Such data is to be used in a way which ensures that the citizens will continue to have confidence in the Regions. Therefore information security must be an integrated part of the service delivered by the Regions to citizens, patients, businesses, co-operators, etc., just as it must be an integrated part of the day-to-day work for employees and other users. The handling of information security by the Regions is to ensure that the patients will get the best possible treatment while their data remains safe.

Sensitive personal data, including health data, is personal and when the Regions process it, they have a special responsibility to ensure a high level of security. Consequently, the Danish Regions have in 2015 established a policy for information security to be implemented by this policy. According to the policy it is important that

- information security is used as a foundation for a continually improving health sector
- the Regions establish a sufficiently high level of information security
- information security and user-friendliness walk hand-in-hand
- all employees understand that their behaviour is the basis for information security
- the Regions cooperate and learn from each other

- the Regions set up requirements for suppliers

The policy defines the following three general areas.

1. *People, Organisation and Processes*

The employees' behaviour in their day-to-day work is very important for information security. It is central that all employees are aware how their behaviour affects information security. It is both a question of how the employees handle technology and IT equipment and of how they treat sensitive personal data. Consequently, the employees must be familiar with legislation, the Regions' own policies, guidelines and instructions – and they must of course also observe them. It is also important that management gives priority to the area. The Regions should therefore establish an organisation which gives priority to information security so that employees and management have good conditions for working with sensitive personal data.

2. *IT Systems and Physical Security*

The Regions' use and handling of sensitive and confidential information shall be conducted in a safe manner and with an appropriate level of security and protection of privacy. Among other things this requires the Regions to handle the information confidentially, to maintain the integrity of data and to change information only after authorisation. Data shall only be available to people who need it, and access shall be secure. This makes technical requirements in connection with development, implementation and operation of IT solutions and to the physical safeguarding of hardware, etc.

3. *Statutory and Contractual Requirements*

The Regions shall ensure that relevant statutory and contractual requirements are observed in the day-to-day work. The Regions must only process citizen data when the necessary statutory basis exists. This element of information security also involves a focus on adding specific contractual requirements regarding data security in the operating and development agreements entered into with suppliers by the Regions.

It is important that citizens, patients, businesses, cooperation partners and other stakeholders are confident that the Regions have established necessary initiatives to safeguard citizen's data and that the Regions administer their sensitive personal data safely and responsibly.

The political guidelines for information security also require the Regions to comply with the ISO 27001 standard as a framework tool for working with information security in the Regions. Together with the information security policy of each Region, the joint regional policy is to support and ensure a consistent security level. This is to be obtained by each Region's establishment, implementation, maintenance and improvement on an ongoing basis of a management system for information security within the framework of the information security standard, ISO 27001.[1]

[1] In this connection, a management system, also referred to as an InformationSecurityManagementSystem (ISMS), reflects the policies, procedures, processes, organisational decision-making procedures and activities which form the Regions' information security control. Each Region has established a structure and framework and work procedures for the information security work.

2. Organisation

To ensure processing and storing of sensitive personal data in accordance with the requirements of the law, it is important to plan the organisation so that it becomes natural in practice to comply with the information security rules. Anchoring in senior management is the initial step in this work.

Each Region must have an unambiguous and written management responsibility for information security, reflecting a structured approach to information security in the organisation. It has to cover the entire organisational level.

Senior management is responsible for making the final decision on a security level in line with risk and importance and the interests of the public. The level must comply with relevant legislative and contractual requirements.

Senior management is responsible for supporting policies, guidelines and instructions and for allocating necessary resources to carry out the work within information security in the Region. It must ensure that the Region's employees have the necessary knowledge of information security.

On the basis of the policies, guidelines and instructions issued by senior management, **line management** is responsible for ensuring that such policies, guidelines and instructions are observed in their own units.

Management must work for a culture in which responsibility in relation to information processing comes naturally for everybody. All **employees** are responsible for contributing to ensuring that the Region's information does not get into the wrong hands. The management is responsible for ensuring that all employees have the necessary knowledge of information security and that the relevant training in information security is available. Similarly, the employees are obliged to familiarise themselves with the information about information security which is made available.

3. Area of Validity

The joint regional information security policy and the information security policy of each Region shall apply where the information, and in particular the sensitive personal data, of the Region is stored or processed. It is of no importance for the area of validity where and how it is stored or processed. The Region's information must only be processed according to agreement with the Region in question. Thus the information security policy applies to:

- **All users**. A user means for example employees, researchers, consultants, members of the Regional Council, pupils, students and others who have temporary or long-term access to the Region's personal data.
- **Partners** who store or have access to or process biological material, paper-based or electronic sensitive personal data according to agreement with the Region. In this connection it is irrelevant whether the partners are located in or outside Denmark.
- **Joint regional partners**. Where several Regions use the same partner or supplier for joint solutions, the joint regional information security policy must be used.

The joint regional information security policy and the information security policy of each Region shall, however, not apply to citizens who have access to their own personal data with secure identification and through system access aimed at citizens.

4. Targets

To comply with the ISO 27001 standard, the Regions have the following joint targets:

To ensure a sufficient and acceptable security level, it is necessary to assess the risks ranging from vulnerability in the individual systems to the risk of being the victim of attacks by hackers.

A. The Region's security level and risks are established on the basis of an overall risk assessment[2]. The risk assessment must
- Create an overview of the risk profile of the Region which constitutes a survey of identified information security risks
- Ensure the preparation and maintenance of a catalogue of identified threats
- Identify the most vulnerable and critical systems
- Ensure management involvement in the definition of the security level
- Create awareness of security in the organisation
- Form the basis of the preparation of an action plan to meet identified threats to the systems.

B. On the basis of each Region's risk assessment, the Region shall establish its own time frame and method for
- preparation and maintenance of a SoA [3]document (Statement of Applicability)
- preparation of policies, guidelines and instructions and supervise compliance
- preparation and test of IT emergency plans and emergency procedures
- preparation and initiation of initiatives creating awareness
- reporting regularly to relevant management levels on information security.

In complying with current legislation, the Regions have the following targets:

C. The current legislation at any time within the area, in particular legislation within the protection of personal data, must be observed in the Regions and by their partners, including by
- ensuring that any processing of sensitive personal data is carried out according to a risk-based approach and in accordance with current legislation
- ensuring that disclosure and handing over of information shall only be carried out according to legislation and data processor agreements
- documenting data flows, security initiatives and control initiatives
- observing technical requirements regarding logging, authorisation and role control
- documenting systematic follow-up of logging
- placing suppliers under an obligation to ensure sufficient and responsible information security levels through requirements and control
- registration of violations or possible violations of information security.

5. Approval

The Joint Regional Information Security Policy is to be approved by the five Regional Councils in 2016.

---

[2] The risk assessment identifies, analyses, and evaluates risks on the basis of the defined context.

[3] SoA can be seen as a statement of the security level actively decided by the organisation, and the reasons for the decision.