Coops IT SECURITY POLICY

1. STATED POLICY AND LEVEL OF IT SECURITY

The IT security policy must at any given time support the core values, vision, and strategic goals of Coop.

The IT security policy and the supporting rules establish the fundamental framework, according to which we work, in order to avoid IT security breakdowns and to be able to handle the incidents that occur in spite of our efforts.

The IT security policy applies to all departments and all employees of Coop Denmark. It applies to anyone who is affiliated with Coop in any way that allows them access to IT resources and thereby acts by the account and risk of Coop.

The executives of Coop are responsible for complying with the current IT security rules. This means that the individual executive is responsible for making sure that their own employees as well as external consultants and temporary workers are informed of the IT security policy of Coop and that they have a basic understanding of how and why it must be complied with. The management of Coop must support the IT security by defining clear guidelines and by showing a visible commitment.

The overall level of IT security of Coop's business is established in the IT security policy.
The level of IT security reflects the risk tolerance as anchored in management of Coop, and it is defined by the implementation of an IT risk assessment in proportion to the risks assessed by breaches of:

- confidentiality
- reliability
- inaccessibility.

The result of the IT risk assessment will be presented to the executive board for approval.

When discussing the possible consequences of risks, this will happen by identifying if breaches of the security can affect the business according to:

- Stategies, where Coop will be unable to undertake important activities
- Economy, where there are substantial financial losses, loss of earnings, or significant fines
- Organisational challenges, where resources have to be unrealistically increased
- Legislation, e.g. violation of regulations regarding personal data, violation of the penal code.

The level of IT security

Coop is one of the largest companies in Denmark and therefore we must live up to the expectations of our surroundings and our members as we play a big part in Danish society.

Coop is a grocery business and it is crucial to Coop that the products come "from earth to table". Translated into IT security, this means that the reliability and accessibility of the product systems and payment systems are of crucial importance. If our systems do not communicate or if data is incorrect, the customer will not be able to purchase the products and the right products will not arrive to the customer.

Our members are the core of our business and we have to maintain their trust. This means that the data of our members must be processed confidentially and according to the Danish Act on Processing of Personal Data. Our reputation with our customers is one of the biggest assets we have in Coop.

Coop will use technology to give our customers a good shopping experience and to establish good processes for business. Therefore our systems must be adapted to meet future requirements and to facilitate everyday life. This means that we must ensure solid architecture, structure, and quality of the systems and the data. This also means that we must ensure a good management of the development processes regardless of whether it happens through internal forces or the job is outsourced.

Coop is a large company with many employees and therefore we must ensure a safe management of user roles and which rights we assign to our IT resources.

Finally, in the field of technology, we must be a professional and forward-looking company that can attract the best technical employees so that we, together, can realise the digital potential of Coop.

2. METHOD AND DEMANDS

As a basis for the IT security implementations, Coop takes the ISO 27001 and ISO 27002 as point of departure.
Where relevant, when it comes to the reception of payment card information in stores, we work in accordance with the Payment Card Industry Data Security Standard (PCI DSS), version 2.0.

Additionally, there are laws and regulations in some areas that may impose specific requirements. This is the case with:

- Processing of personal data, including information about employees, customers, and members.
- Handling of bonus and dividend, this must be processed as a substitute payment free of all charges.

The applications and data of Coop are considered a critical resource for Coop. Therefore, operational reliability, quality, and well-documented operational process are emphasized.

The comprehensive IT security concept of Coop contains the following:

- The IT security policy of Coop, which lays down the general framework in terms of management. It is approved at executive level.
- IT risk assessment
- IT contingency plan
- Other regulations and procedures produced by Information Security

All IT safety procedures and instructions will be drawn up and maintained by the persons in charge of the given IT services. Fundamental and strategic matters will be accomplished by Coop Technology Information Security.

3. THE IT SECURITY ORGANISATION AND RESPONSIBILITIES

Coop executive board has the overall responsibility for the IT security and has delegated the daily responsibility for the IT security to Coop Technology Information Security.

Information Security operates the Technology Risk Committee (Teknologi Risiko Komiteen, TRK), which is responsible for implementing the required IT security level and that it is complied with across the organisation. The TRK is a special committee with reference to the ERM board (Enterprise Risk Management), which has the broad perspective across all types of risks.

3.1. Employees

It must be ensured that each employee receives the leaflet “Sikkerhedsselen” (The Safety Belt) which gives a general introduction to the expectations that must be met regarding the IT security.

3.2. Business partners

When Coop makes use of external consultants and business partners, it must be ensured that internal Coop employees undertake the management role and are at the head of all operational decisions.

If it is considered necessary for one of the external business partners of Coop to get access to Coop's network, they can be granted access. However, the business partner must only be granted access to the systems in which they have a work-related need for access.

Before the access to Coop's network is granted, the external consultant must sign a confidentiality clause (Coop's Non Disclosure Agreement – NDA).

If access to the system only takes place under surveillance of a Coop employee, it is sufficient that the business partner, on behalf of the employee, has signed an agreement (NDA), where the business partner ensures that the above-mentioned obligations are complied with.

4. IT contingency plan

Catastrophes are sought be avoided through well-structured, physical protection and surveillance of buildings, technical installations, and IT equipment. The proportions of these precautions will be decided based on a trade-off between risks and the costs of protection and will be implemented in the SLAs.

Coop's technological preparedness should include:

- How contingency is handled and the correlation between existing task force-handling via ServiceDesk.
- Re-establishment of temporary/permanent solutions.
- The contingency plans must be updated and tested regularly.

5. Access to systems and applications

For all operating systems there must be specific guidelines and procedures of the administration of users and access.

- Coop protects data and IT systems on the principle “Need to Protect”. This means that a user who has permission to access a system by default gets access to the entire system. If further limitations of user access should be implemented, there must be an operational reason.
- Coop Technology must be in full control of the user administration on all the group IT systems. This means that there must be a model of authorisation which ensures that decentralised, and thereby unauthorised, changes will be overwritten.
- Coop must have a central and automatic process for user administration.
- Coop must keep access to Coop's own systems and Coop bank A/S completely seperated.
- Persons who are granted access to an IT system are held responsible for the use and misuse of the access.
- There must be processes for manual granting of access in cases where the normal criteria for granting of access prove to be insufficient, in which cases Coop must follow the principles mentioned below.

6. Change management

Coop's procedure of changes (Change management) must be followed during any changes in applications, IT services and infrastructure, and the granting of access to any of these.

7. Physical locations

Specific rules and procedures for the regulation and accessibility must be formulated and implemented by the time of the occupancy of buildings.

If an activity is included in an outsourcing agreement, it must be ensured in the contractual basis that the NDA and IT security policy of Coop are complied with, e.g. by requiring that the supplier carries out different inspections and reports about the efficiency of these, for instance in a suitable audit report.

8. Monitoring

The IT security policy will be revised every third year and when bigger changes are made. The policy must be approved at Coop Amba level.

This is a translated version of the IT Security Policy written in Danish.