Pohjola Insurance

Safety regulations for data centres, S710

Your obligation to prevent damage, valid as of 1 January 2024

Welcome to the safety regulations!

In these safety regulations, we explain what your company must do and take into consideration with respect to data centres.

Read the regulations carefully. If you do not comply with the regulations, we may reduce or deny your insurance compensation.

These safety regulations are part of your insurance contract.

Your insurance contract consists of the policy document, insurance terms and conditions, safety regulations, and the general contract terms and conditions.

The **policy document** lists your company's insurance policies and the terms and conditions applicable to them.

The **insurance terms and conditions** describe the terms under which your property is insured.

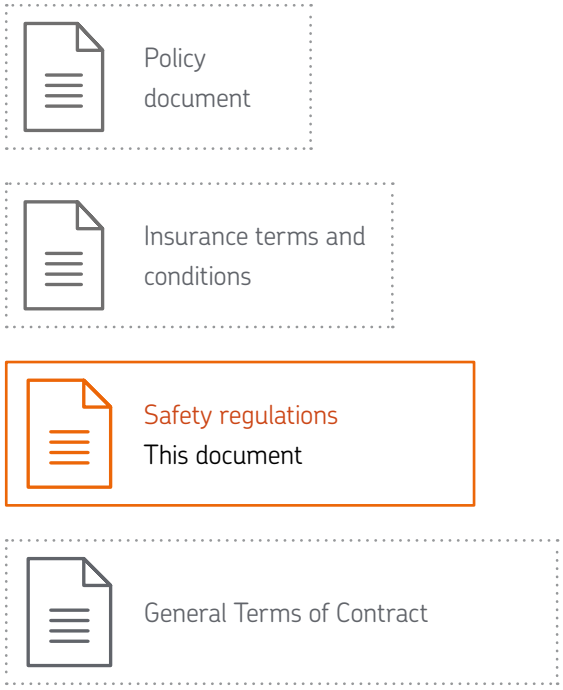
These safety regulations describe your obligations to prevent damage.

Pohjola Insurance's general terms of contract contain general provisions related to your insurance.

We interpret the policy document, insurance terms and conditions, safety regulations, and general contract terms and conditions as a whole.

Please note that the following safety regulations also apply to your insurance contract:

- Daily Fire Prevention S411
- Prevention of Electrical Fires S331



- Automatic Fire Alarms S821
- Cyber Insurance S711
- Safety Regulations for Break-in Protection 1, S851
- Safety Regulations for Break-in Protection 2, S852
- Safety Regulations for Break-in Protection 3, S853

CONTENTS

1 Purpose of the safety regulations: prevention of damage to data centres

These safety regulations set out the requirements for the safety and security of data centres.

Follow these safety regulations in industries and companies that involve the use of data centres, such as server rooms, server hotels, communication stations, IT network control rooms or other facilities used to house servers.

- The information presented in these safety regulations will help minimise some of the most common risks to which an organisation's data centre may be subjected.
- The purpose of these safety regulations is to highlight the principles and best practices related to the construction and use of data centres.

✓ **Ensure** that the accessories and hardware referred to in these safety regulations are kept operational and maintained and checked appropriately.

✓ **Prepare** an appropriate maintenance programme.

Note: These regulations do not address protection against threats that may typically occur in emergency conditions such as those caused by radiation, biological weapons, EMP and HPM weapons, or harmful gases.

Your company has an obligation to ensure that

- the safety regulations are followed in all activities carried out by the policyholder, insured persons or parties comparable to insured persons.

Always take the criticality of the organisation's or operation's IT systems and the data contained in systems and their importance into account in the planning, sourcing and implementation of information security.

- Organisations that are especially dependent on information technology are required to observe a higher level of security.
- An organisation or function particularly dependent on information technology would not manage for more than 24 hours without information systems.
- Dependence on information technology is considered lower if an organisation or function can manage to operate without information systems with relatively little disturbance between 24 hours and several days.

2 Requirements for protection against most common risks

> ⓘ Pay particular attention to hardware and data centres used to process highly classified information. These are subject to higher security requirements than hardware and data centres with a lower security level.

2.1 Backup arrangements and business continuity plans

- ✓ **Follow** these safety regulations for data centres S710.
- ✓ **Prepare** a business continuity plan when necessary, as well as separate data processing continuity, recovery and contingency plans that address the following matters:
    - How operations can be continued
        - ounder emergency conditions
        - in different business locations
        - on a smaller scale than under normal conditions
        - in a separate backup server room and data centre or another backup facility prepared in advance in the case of data centres with a high security classification.
- ✓ **Ensure** that the backup data centre is a physically separate location where operations may continue under emergency conditions.
- ✓ **Ensure** that the necessary personnel to start up the backup data centre has been assigned and reserved.
- ✓ **Ensure** that the backup systems have up-to-date data and reservations for data communication connections at the backup site.
- ✓ **Instruct** personnel on the operations and ensure that personnel receive training in accordance with the plans.

2.2 Instructions and alarms during disturbances

- ✓ **Direct** alarms to a centralised control point or to a person who is in charge of security in the premises.
- ✓ **Ensure** that the person receiving the alarm has clear instructions for how to act in the event of alarms.
- ✓ **Test** alarms regularly to ensure their functionality.
- ✓ **Train** personnel responsible for receiving alarms.

3 Risks and protection against them

Some common risks to data centres containing IT equipment include:

- Data security breach, data theft and human error
- Fire and explosion, water damage and flooding
- Power outage, voltage disturbance, temperature rise
- Equipment breakdown, equipment theft, criminal damage
- Damage caused by EMP and HPM
- Damage caused by chemical substances, radiation accident

3.1 Protection against theft, vandalism and break-in

- ✓ **Prevent** unauthorised access to data centres.

- ✓ **Ensure** that only separately designated IT personnel and equipment maintenance and cleaning personnel have access to data centres, and with proof of identity and a valid reason for the visit.
- ✓ **Monitor** access to data centres taking into account the criticality of the premises.
- ✓ **Ensure** that the premises are cleaned and maintained only while the relevant responsible personnel are present.
- ✓ **Arrange** access control if necessary so that entry to and exit from the premises is logged electronically or recorded by another means.
- ✓ **Ensure** the management of various forms of vandalism and criminal damage in the structural design of data centres. Technical aids may include locking, an access control system, control of irregular working hours, reporting on deviations and break-in detection systems.
- ✓ In access control, **ensure** that authorised access is as easy as possible while preventing any unauthorised access. Any equipment brought into the premises by visitors must be available for inspection if necessary.
- ✓ **Arrange** access control so that personnel only have access to premises necessary for the performance of their duties.
- ✓ **Ensure** that access keys or cards and related security codes, ID cards and detailed written access instructions are only granted against the person's signed acknowledgement of receipt.

ⓘ Data centres must be constructed of materials that provide good protection against any break-in. Any unmanned data centre should be located in the middle of a building in a windowless room, and compartmented to be separate from other data centre premises.

Wall, ceiling and floor structures must be sufficiently strong and of such construction that it is impossible to force an entry into the space without using tools to break the structures. Such materials include concrete, other aggregate-based materials, metal or composite structures with safety features designed for data centres.

- ✓ **Ensure** that it is impossible to remove the structure or any part of it from the outside without breaking it. A Class 3 anti-burglary wall meets the above requirements (see Safety regulations for break-in protection 1).
- ✓ **Ensure** that doors to the premises are generally kept locked at all times.
    - When the premises are vacant, locks must be kept double-locked, and the panic bolt on double doors locked.
    - However, the safety lock must be kept open when people are in the premises to allow people to exit in an emergency.
    - On the inside of the exit doors, there must be a handle or a twist knob with a plastic cover in case of emergencies.
- ✓ **Equip** data centres of a high protection level with a crime detection system approved by insurance companies.
- ✓ **Organise** surveillance of the premises with at least perimeter and premises security using magnetic door sensors and motion detectors. Ensure that the motion detectors are protected against covering and the magnetic sensors sound an alarm if a door is left open. Connect the system to a local alert system in the data centre's interior and exterior.
- ✓ **Ensure** that the crime detection centre is of a type approved by insurance companies and sends an alarm to an emergency centre that is manned around the clock. Ensure that the alert notification connection is monitored and duplicated at least once.

3.2 Structural protection against intrusion into information systems and data connections

ⓘ The purpose of protecting data communications is to ensure their functionality.

Effective protection prevents:

- unauthorised intrusion into the information system and exposes unauthorised intrusion attempts
- third parties from accessing transferred data
- abuse of possible data that has fallen into the wrong hands
- entry of false data into the information system.

✓ **Implement** data connections on high-security sites using at least two channels that are independent of each other and led into separate cross-connection points that can be operated jointly and used to transfer the connection.

✓ **Ensure** that any changes in the information networks of data centres are approved by the management in charge of data communications or the information system. Any changes must be documented and tested before implementation.

✓ **Divide** the responsibilities related to information security clearly. Ensure and monitor that instructions and agreed policies are followed.

✓ **Use** optical fibre for data transfers whenever possible:

- Optical fibre does not react to electromagnetic radiation and has a moderate tolerance of fire.
- Optical fibre is also difficult to wiretap.
- On a case-by-case basis, the requirement to encrypt data transmitted via an optical fibre can be replaced by physical access control and monitoring methods if the premises are fully under the user's control.
- The advantages of optical fibre include a good transmission speed, a large bandwidth, durability, and a small size and weight.

3.3 Fire protection

✓ **Equip** the data centre with a fire detection system. Data centres with a high level of protection must have not only fire detection equipment but also air sample detectors and automatic fire extinguishing equipment.

✓ **Place** the building automation, fire protection and other systems serving the data centre outside the premises so that maintenance can be carried out without outsiders accessing the data centre.

✓ **Prepare** a maintenance plan for the fire detection system in the data centre. Ensure that equipment maintenance is organised so that the equipment meets its requirements throughout its useful life.

✓ **Perform** thermal imaging of main distribution boards and subpanels regularly to prevent electrical fires.

Fire load and cleaning of premises

✓ **Prepare** a cleaning plan and ensure that it is followed regularly. This way, dust and other additional fire load do not increase the risk of fire or equipment failure.

✓ **Do not** store any unnecessary materials or flammable liquids in the data centre. Aerosol cans used to clean equipment must be stored in separate metal cabinets.

Structural protection

- ✓ **Ensure** that lead-throughs in the premises are sealed using appropriate and approved fire foam depending on the fire resistance of the structure.
- ✓ **Keep** doors closed at all times. Ensure that the fire resistance period of fire compartment doors is as long as that of compartment walls and structures.

Fire detection

- ✓ **Equip** the premises as well as any space below the installation floor with smoke detectors in accordance with the applicable installation instructions. Connect the detectors to the property's fire alarm centre capable of shutting down ventilation in the property in the event of a fire alarm.
- ✓ **Find out** how shutting down ventilation equipment affects the temperature in premises used to store equipment susceptible to temperature rises.

Automatic fire extinguishing system and first-aid extinguishing equipment

- ✓ **Avoid** installing aerosol systems in the data centre.
- ✓ **Follow** the applicable installation and design instructions of the gaseous fire suppression system when installing the system. Using pressure differential valves or other means, ensure that released gas does not damage the equipment or structures in the data centre.
- ✓ **Equip** the data centre with a sufficient amount of first-aid extinguishing equipment and ensure that the equipment is inspected and serviced regularly. Place at least one CO2 hand-held fire extinguisher for every starting 300 m2 of floor area and outside the front door. Mark the hand-held fire extinguishers clearly and keep the space in front of them clear of obstructions.
- ✓ **Ensure** that personnel working in the premises have received training in first-aid fire extinguishing.

3.4 Protection against heat and smoke

- ✓ **Equip** the data centre with a separate ventilation system. Place the ventilation equipment in a separate fire compartment. Ensure that air pressure is higher in the data centre than in the premises around it.
- ✓ **Separate** the ventilation of the data centre from other ventilation using fire dampers equipped with smoke detectors if an entirely separate ventilation system is impossible.
- ✓ **Ensure** that ventilation equipment shuts off automatically if the fire detection or suppression system is activated. Ensure that ventilation can also be shut off manually if necessary. Place the manual shut-off switch in the same space as the main power switch.
- ✓ **Place** ventilation equipment in a separate ventilation unit room.
- ✓ **Ensure** that ventilation flues are made of non-flammable materials and equip the flues with automatic fire dampers.
- ✓ **Prevent** smoke travelling between fire compartments via ventilation ducts.

3.5 Protection against water damage

ⓘ In planning protection against water damage, pay attention to the location of the data centre on the property. In practice, the design of the data centre must take into account and prevent, where possible, risks of water damage from below and above the premises and from adjacent rooms and pipes placed in the data centre. The data centre must be built above the ground floor, or the equipment must be placed on a raised platform. The minimum height for installations susceptible to water damage must be higher than the height needed to control water leaks. Do not install pipes in the data centre which would cause water damage in the event of breakage.

- ✓ **Equip** the data centre with water damage alarm sensors.
- ✓ **Equip** any floor drains with back stop valves to prevent water entering the premises.
- ✓ **Ensure** that the automatic drainage system in the premises is independent of external power sources.
- ✓ **Equip** the data centre with an anti-leak drainage system independent of external power sources if the data centre is below groundwater level.
- ✓ **Place** hardware in the data centre so that it is not susceptible to failures in pipes in the ceiling of the premises or damage caused by condensation.
- ✓ **Install** waterproofing in the ceiling above the data centre.
- ✓ **Ensure** that the ceiling structures of the data centre, premises containing data communication equipment and control rooms are clear of obstructions. Ensure that the ceiling and walls of the data centre are only used for piping that is required for the safe operation of the premises. If the piping cannot be moved, it must be encased, or any critical equipment stored below them protected with a waterproof and non-flammable lowered covering, away from which any leaked water can be safely redirected. Install leakage detection alarms in the covering.

3.6 Protection against dust

- ✓ **Ensure** the premises are cleaned regularly. Pay particular attention to structures that may gather dust.
- ✓ **Ensure** that intake air is filtered and clean.
- ✓ **Clean** ventilation ducts regularly.
- ✓ **Ensure** that floor and wall materials are kept free of dust.

3.7 Protection against vibration

- ✓ **Ensure** that data centre racks are equipped with alarm sensors in case the doors are opened if the rack is used to store highly classified information.
- ✓ **Ensure** that racks are sufficiently fastened in place and equipped with vibration dampeners. In demanding conditions, servers must be installed on specialised racks equipped with spring suspension.

3.8 Protection against chemical effects

- ✓ **Equip** air ventilation equipment with gas and particle filters.
- ✓ **Take into account** the effects of airborne chemicals on the operation of the filters in the planning of ventilation equipment.
- ✓ **Ensure** that the premises are sufficiently sealed for pressurisation.
- ✓ **Shield** the data centre's doors, hatches, equipment, ducts, pipes and their fastenings, and other parts susceptible to corrosion.

3.9 Protection against electrical grid disruptions

- ✓ **Ensure** uninterrupted power supply by means of backup power sources in data centres with a high level of protection.
- ✓ **Test** the operation of any backup power generators regularly. Place the backup power generators and their fuel in a separate fire compartment. Test and service the equipment regularly.
- ✓ **Ensure** that the backup power is sufficient for all electric equipment in the data centre, ventilation, cooling and lighting.
- ✓ Also **ensure** the power supply for the separate ventilation system in the data centre.

ⓘ The following are suitable for protecting data centres and equipment against electrical disturbances: isolation transformers; power line filters; voltage stabilisers; and equipment that secures an uninterrupted power supply.

Use uninterrupted power supply (UPS) in all data centres to ensure power supply. Scale the UPS equipment to function for as long as necessary for the disruption to end, or until the backup power supply is online. After this, UPS acts as a filter between the power grid and the equipment.

3.10 Protection against equipment breakage

- ✓ **Sign** a maintenance agreement with the manufacturer or importer of the IT and ventilation equipment
  - **Ensure** that service and maintenance is carried out in accordance with the instructions. Keep logs of all maintenance work.
- ✓ **Ensure** that the system must be backed up in the event of equipment breakage.
- ✓ **Place** the data centre's main power near the exit in a place where it is easy to see and reach. Mark the location of the main power switch clearly and protect it to ensure that power cannot be switched off or on by accident. The main power switch must switch off all power in the data centre.

ⓘ The data centre's temperature and humidity must be suitable for the equipment. As a general rule, follow the equipment manufacturers' recommendations. If these are unavailable, use the following generally accepted values: the temperature in the data centre should be at least +20 °C and no more than +26 °C. Relative humidity must be between 40% and 60%.

3.11 Protection against data loss

- ✓ **Store** data media in the data centre in separate operational and backup archives located in physically separate premises.
- ✓ **Place** the digital waste storage in a separate fire compartment.
- ✓ **Prepare** for emergency conditions by taking backups regularly and storing them separately from the equipment.

ⓘ If the environment of the organisation or operation involves a risk of electromagnetic radiation, the radiation tolerance of the systems and level of electromagnetic protection of the equipment must be determined based on the maximum exposure to radiation.

3.12 Protection against static electricity

- ✓ **Use** a semiconducting work surface and a static control wrist strap when performing any maintenance in a data centre. Antistatic flooring material ensures protection against frictional electricity.
- ✓ **Ensure** sufficient air humidity to reduce the amount of static electricity.
- ✓ **Install** electrical cables separately from data cables. Direct electrical cables to the data centre from more than one point of entry.

3.13 Drawings and device registers

- ✓ **Keep** a register of devices in the data centre.
- ✓ **Ensure** that the drawings and description of the data communication network are up to date.

- ✓ **Ensure** that the description and drawings of the data communication network are available only to a limited number of necessary personnel at all times during the design phase and later.
- ✓ **Ensure** that the field log is signed during the delivery inspection and stored in a secure place with other data centre documentation.
- ✓ **Make sure** that all devices are documented, and that the connection diagrams, including any recorded changes, are up to date.
- ✓ **Mark** cross-connections and cables clearly.

3.14 Outsourced data centres

- ✓ **Sign** the necessary agreements on the service level, audits, quality and backup storage of data centres and services that are outsourced to third party premises outside the organisation.
- ✓ **Include** a separate description of the service provider's data centre security and business continuity plans in the agreements if necessary.

3.15 Risk identification and assessment

ⓘ Prepare a risk assessment of potential risks to the data centre. Risks can be ranked into different probability categories based on their probability and severity, for example. This means that a piece of information in a low-level data centre may be a crucial piece of a larger significant whole.

The purpose of risk assessment is to identify the risks to operations and their potential effects. The purpose of the assessment is to determine the risk's probability and the extent of potential damage. Identification of risk factors and the assessment of their risks to the organisation's operation and data processing form the basis of all information security measures.

By following these regulations, you will ensure the security of premises and avoid unpleasant surprises in the event of an insurance claim.

Thank you for taking the time to read these safety regulations!

Pohjola Insurance Ltd, Business ID: 1458359-3

Helsinki, Gebhardinaukio 1, 00013 OP, Finland
Domicile: Helsinki, main line of business: non-life insurance companies
Regulatory authority: Financial Supervisory Authority, www.fiva.fi

Pohjola Insurance