Safety Regulation

Valid as of 1 January 2018.

Data centres S710

290101e 01.18

1 Purpose

These safety regulations are to be included in the insurance contract to supplement the actual insurance terms and conditions. These safety regulations include technical safety regulations and advice which, provided that they are complied with, may prevent loss and damage from occurring and diminish their volume.

2 Obligation to comply with safety regulations

These safety regulations are part of the insurance contract. Both the policyholder and the insured must comply with the safety regulations and its provisions. If the safety regulations are not complied with, the compensation may be reduced or completely denied in accordance with the Insurance Contracts Act.

The policyholder must ensure that people working in the company are familiar with the contents of these safety regulations.

It is the organisation's or function's criticality or the information contained in the systems that determine the level of data centre protection or any additional need for protection.

Organisations or functions particularly dependent on information technology must have a higher level of protection than those that depend less on information technology. On 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.

Equipment and data centres processing highly sensitive information are required to have a better level of protection than equipment and those dealing with less sensitive information.

The following additional safety regulations apply to data centres:

- Daily fire prevention S411
- Prevention of electric fires S331
- Automatic fire alarms S821
- Cyber S711
- Safety regulations for break-in protection 1, S850
- Safety regulations for break-in protection 2, S850
- Safety regulations for break-in protection 3, S853

3 General

The matters is these safety regulations will help reduce some of the commonest risks that an organisation's data centre may be subjected to. Information data centres generally refer to a computer room, communication station, information network control or management room or other separate space containing servers. These guidelines do not deal with protection against threats that may typically occur in emergency conditions, such as radiation, biological weapons, EMP and HPM weapons or harmful gases.

The purpose of these safety regulations is to highlight the principles and practices of matters relating to the design, construction and use of server rooms or other ICT premises.

The equipment and machinery referred to in these safety regulations must be kept operational and both maintained and checked appropriately. A maintenance plan must be made for this.

4. Risks and protection against them

4.1 Risks with ICT data centres

The commonest risks to data centres include:

- data security breach, data theft
- fire and explosion
- water damage, flooding
- power cut
- voltage disturbance
- equipment breakage
- temperature rise
- equipment theft
- human error
- criminal damage
- damage caused by EMP and HPM
- damage caused by chemical substances
- radiation accident.

4.2 Protection against theft, vandalism and break-in.

Unauthorised access to data centres must be prevented. In addition to designated IT staff, only equipment maintenance persons and cleaners may be allowed into data centres and the latter only after they have proved their identity and indicated the necessity for the visit. Any visits will be supervised, considering the importance of the location.

Access to the data centre must be arranged whenever necessary so that nobody can get in or out without being registered (electronic log).

When designing the data centre structures, attention should be paid to the management of various types of vandalism and crime risks. Technical aids may include locking, access control system, control over irregular working hours and reporting on deviations and break-in detection systems.

The objective with access control arrangements is that authorised access is as fluent as possible while preventing any unauthorised access. Access keys or cards and related security codes, ID cards and detailed written access instructions will only be given to people who sign for them.

Data centres must be constructed of material that give 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.

The 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. It must not be possible to remove the construction or any part of it from the outside without breaking it. A Class 3 anti-burglar wall must fulfil the above requirements.

As a rule, the doors to the data centre must be kept locked. If there are not normally people in the space, the locks are to be double-locked and the panic bolt on double doors is to be locked.

However, the safety lock must be kept open when people are in the premises in order 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.

The data centre of high protection level must be equipped with a crime detection system approved by insurance companies. Monitoring must focus on at least the building and the data centre. The building is monitored by means of, for example, magnetic contacts on doors, and the data centre by means of motion detectors. The motion detectors must have be equipped with an anti-mask detection feature. The magnetic contacts must set off an alarm if the door is left or wedged open.

The crime detection centre must be at least of the type approved by insurance companies, of at least Class 3 (SFS-EN 50131-1) that sends an alarm to an emergency centre that is manned around the clock. Alarm transmission must be implemented at least duplicated, and the recommendation is a supervised alarm transmission connection. The system must also have a local alarm (a siren) both inside and outside the premises.

Any equipment brought into the premises by visitors must be checked to prevent sabotage attempts.

4.3 Preparation against fire

The data centre should be provided with fire detection equipment. 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. Any automation, fire and other equipment serving the data centre must be placed outside the data centre, so that no unauthorised persons will enter the data centre during maintenance.

The owner or holder is responsible for ensuring that there is a maintenance programme for the data centre's IT equipment. Repair and maintenance must be organised according to the maintenance manual of each piece of equipment to ensure that the equipment fulfils its requirements throughout their life. To minimise electrical fires in the main distribution board or subpanels, they must be examined by means of thermal imaging to detect any damaged or outdated cables.

Fire load and cleanliness of premises

The data centre must be cleaned regularly according to the cleaning programme so that neither dust nor any extra fire load will increase the fire or equipment breakage risk. Any raised access floors are cleaned at least one a year.

The data centre is not a storage room, so any extraneous flammable material such as unused equipment, paper products or connector cables must be taken out.

No flammable liquids may be kept in the data centre. Flammable liquids must be stored in another space designated for them. Aerosol cans used, for example, to clean equipment, must be kept in a lockable metal cupboard designated for them.

Ensuring structural protection

Any bushings leading to the data centre are examined after installation with a suitable and approved paste that corresponds with the structure's fire resistance. The data centre doors may never be left open. The cable and pipe bushings in compartment walls and ceilings must have the same fire resistance as the walls and ceilings. The fire resistance period of compartment doors and data centre doors must be as long as that of compartment walls.

Fire detection

Data centres and any the space under raised access floors are equipped with a sufficient number of smoke detectors that conform with design and installation instructions for fire detectors. The fire detectors are connected to the property's fire detection centre, which must stop the property's ventilation in the event of fire to prevent smoke from getting from one fire compartment to another. Because a temperature rise in the data centre may damage the computers, it must be estimated separately how the data centre will operate if the standard air conditioning equipment is turned off.

Automatic fire extinguishing equipment

If gaseous fire suppression equipment has been installed in the data centre because of the latter's critical nature, the installation must conform to installation and design instructions of such equipment. We do not recommend the installation of aerosol systems in data centres.

When installing gaseous fire suppression equipment, the effect of gases being released into the data centre structures must be taken into account, with any potential breakage caused by the pressure prevented by means of pressure differential valves.

First-aid extinguishing equipment

The data centre is equipped with a sufficient number of fire extinguishers which are maintained and checked regularly; for each new 300 m^2 of floor area and on the outside of the door, there must be at least one CO2 hand-held fire extinguisher. People working in the data centre have been taught to use hand-held fire extinguishers in a safe way.

The hand-held fire extinguishers must be clearly marked and the area in front of them kept clear.

4.4 Protection against heat and smoke

The data centre must be equipped with a separate air ventilation system, the machinery of which must be located in a separate fire compartment. Ventilation must be arranged so that the air pressure is higher in the data centre than in the premises around it. If an entirely separate ventilation system cannot be implemented for the data centre, the data centre's ventilation must be kept separate from other ventilation by means of fire dampers controlled by smoke detectors. Any air ventilation equipment must shut down automatically when fire alarms or extinguishing equipment are activated. It must also be possible to shut down the equipment manually. The switch must be located in the same place as the main switch for the data centre.

Air ventilation equipment must be located in a separate ventilation unit room. Ventilation ducts must be made of non-flammable materials and equipped with automatic fire dampers.

Any smoke must be prevented from getting through the ventilation system from one fire compartment to the next.

4.5 Protection against water damage

Pipes may not be laid in the data centre in a way that, should they break, would result in water damage. Data centres must be equipped with sensors that alert in case of water damage. The premises must be built above ground floor or the equipment must be on a raised platform. Alternatively, the minimum height for any electrical installations and any other installations susceptible to water damage must be higher than the height needed to control the water leak. If the data centre has floor gullies, they must be equipped with a non-return valve to prevent water from getting in through them.

When building a data centre below the average level of groundwater, the data centre must have equipment for leakage water removal that is independent of an external power supply.

Equipment may not be placed directly under cooling units nor under pipes that lead to such in order to prevent leakage damage caused by any failures or condensed water.

Water removal must be independent of any external power source.

The ceiling immediately above the server room should, if possible, be waterproofed already during construction or during any renovation.

The ceiling structures of the server room, rooms containing telecommunications equipment and the control room must be bare, with no other pipes containing liquids on the ceiling or walls than are required for the safe operation of such special rooms. However, if there are pipes containing liquids on the ceiling or walls and they cannot be removed or the server room moved elsewhere with reasonable effort, the pipes must be boxed in or any server equipment below them protected with a waterproof and non-flammable dropped ceiling.

When installing the ceiling, it must be ensured that any water leaking on the dropped ceiling must run safely off it.

A leak detector must be installed on the upper side of the dropped ceiling, alerting a designated person immediately.

When installing a data centre, you must take into account anything above it (such toilets and washrooms, water-circulation central heating, any production processes, roof) and potential leak risks or water damage caused by water used to put out a fire (water from sprinkler or fire brigade hoses).

4.6 Protection against dust

The surface material of the floor or walls may not create dust, and incoming air must be filtered. The air ventilation ducts must be cleaned regularly to ensure that no dust accumulates in them. The room must be cleaned regularly, remembering structures where dust may accumulate.

4.7 Protection against vibration

In order to protect against vibration, the equipment shelves and cabinets must be firmly fixed in place and provided with vibration dampers. If necessary, servers in demanding conditions must be installed into racks which rest on springs that dampen any shocks and vibration. Depending on the importance of information processed, you may also used lockable cabinets equipped with tamper switches.

4.8 Protection against chemical effects

The design of doors and air ventilation equipment filters must take into account the effect of any chemicals on the operation of the filters. Air ventilation equipment must be equipped with gas and particle filters. The area must be sealed to enable overpressure.

The data centre doors, hatches, equipment, ducts, pipes and their supports and other parts and accessories susceptible to corrosion must be protected appropriately.

4.9 Protection against electrical network disturbances

Premises with a high level of protection must ensure an uninterrupted supply of electricity by means of backup equipment. If auxiliary power generators are used, their operation must be tested at regular intervals. Any auxiliary power machinery must be located in a fire compartment of its own, as must be the fuel needed for them. The equipment must be tested and maintained regularly to ensure automatic operation. The auxiliary power must be sufficient for all the equipment, air ventilation, air conditioning and lighting.

The following are suitable for protecting data centres and equipment in them against electrical disturbances: isolation transformers, power line filters, mains voltage stabilisers and equipment that secure an uninterrupted power supply. Electricity supply must also be ensured for the data centre's separate air conditioning.

Uninterrupted power supply (UPS) equipment are recommended to be used for all data centres. The UPS equipment must be dimensioned to operate for as long as long as the auxiliary power starts working or the disturbance is over. Even after this, UPS will act as a filter between the electricity grid and the equipment.

4.10 Protection against equipment breakage

Breakage of IT equipment and air conditioning equipment and their accessories must be prepared against by making a maintenance agreement with the manufacturer or importer. Preventive maintenance must be carried out according to the instructions given by the manufacturer or importer. The system must be backed up in case of equipment breakage. A log must be kept of all maintenance work.

The data centre's main power switch must be located near the exit in a place where it is easy to see and reach. The main power switch must be marked clearly and protected in a way 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 using the equipment. As a rule, the equipment manufacturers' recommendations must be followed. If such are not available, the following generally accepted values should be observed: the temperature in the data centre should be at least +20 °C and no more than +26 °C. Relative humidity must be 40–60%.

4.11 Protection against misuse by staff

The data centre must be cleaned and maintained only when staff is present. Data centres must have an access control log. Staff should only have access to the premises during their working hours and only to premises where they need to be for their work.

4.12 Protection against data loss

The data centre's data devices are kept in a separate working archive and backup archive, located separately. Data waste must be stored in a separate fire compartment. Emergency conditions can be prepared for by taking safe copies regularly and keeping them separate from the equipment.

4.13 Protection against microwave-frequency electromagnetic radiation

If there is danger of electromagnetic radiation in the organisation's or function's operating environment, the potential level of such radiation must be used to determine the systems' tolerance level and the necessary protection level for the equipment, using the premises' protection level as parameter, or to determine the premises' requirements on the basis of the extent the equipment can withstand electromagnetic radiation.

4.14 Structural protection against intrusion into the information systems and data connection

Data connections in high-security targets must be built using at least two channels that are independent of each other and led into separate cross-connection points, either of which can be used depending on the situation.

The purpose of protecting data communication consists of the following:

- Preventing unauthorised intrusion into the information system
- Exposing any unauthorised intrusion attempts
- Preventing information from getting into the possession of outsiders and preventing the use of any such information
- Preventing false information from being fed into the information system.

Any changes in the information network must be approved by the management in charge of data communications or the information system. Any changes must be documented before implementation. Risks can be managed by dividing responsibilities clearly about ensuring secure data communication and supervising that agreed methods are followed.

Optical fibre must be used as much as possible in the cabling. Optical cables do not react in any way to electromagnetic radiation and can withstand a reasonable amount of fire load.

Optical cables are difficult to wiretap, requiring physical access to the cable. For this reason, the encryption requirement for data communication can be reviewed case by case and if the premises are under your full control, physical access control and supervision methods can be deemed sufficient. Optical cables should also be favoured because of their transfer speed, high bandwidth, durability and small size and weight.

4.15 Protection against static electricity

When performing any maintenance in a data centre, a semiconducting work surface and a static control wrist strap must be used. Antistatic flooring material will ensure protection against frictional electricity. The correct air humidity (air conditioning) will reduce the creation of static electricity.

Electric cables must be installed separate from data cables and run into the data centre from more than one point.

4.16 Instructions and alarms during disturbances

Alarms are directed to a centralised control point or to a person who is in charge of security in the premises. The person receiving the alarm must have clear instructions on how to act in various situations.

Alarms must be tested to make sure they work and to train the staff that receive the alarms.

4.17 Backup arrangements and recovery

If the continuity requirements of the organisation so demand, the organisation must have up-to-date continuity, recovery and contingency plans for emergency conditions and situations. These plans will enable operations to continue perhaps in a different location or at a scale that is more limited than normally.

The design of high-security data centres must take into account any need to continue operations in a separate back-up centre or other prepared location.

The back-up centre is a physically separate location where operations may continue under emergency conditions. Staff must be allocated to start up operations, and up-to-date information must be available in the back-up system to continue operations.

The necessary data connections for the back-up centre must also be reserved. Instructions must be provided for operations, and exercises must be organised according to the continuity and contingency plans.

4.18 Drawings and device registers

A device register must be maintained of equipment in the data centre, and the information network drawings must be kept up to date at all times.

Distribution of the drawings must already at the design stage be as limited as possible so as not to compromise the security of any solution. The field log is signed during the delivery inspection and then kept in a safe along with the other data centre documents.

All equipment must be documented and the connection diagrams be kept up to date along with change history. Cross-connections and cables must be marked unambiguously.

4.19 Outsourced data centres

Today many IT services have been outsourced to subcontractors outside the organisation's own premises. Agreements must be made for these premises in terms of service level, auditing and storage of data back-ups. The agreements may contain a separate description of the service provider's data centre security and contingency plan, which will be helpful in any audit.

4.20 Threat investigation and assessment

The investigation and assessment of threats to IT data centres may be carried out from the viewpoint of the information system to be protected. Threats can be placed into different probability categories on the basis of, for example, their frequency and size. This means that in an individual case, a piece of information in a low-level data centre may be a crucial piece of a larger, meaningful picture.

The purpose of threat assessment is to find out what the operational threats are and what kind of risks they can grow into. The purpose of the assessment is to determine the risk's probability and the extent of potential damage. Identification of threats and the assessment of their risks to the organisation's operation and data processing form the basis for all data security measures.