European Guideline

CFPA-E Guideline No 14:2007

Fire protection in Information Technology Facilities

CFPA EUROPE

European Guideline

FOREWORD

The European fire protection associations have decided to produce common guidelines in order to achieve similar interpretation in European countries and to give examples of acceptable solutions, concepts and models. The Confederation of Fire Protection Associations in Europe (CFPA E) has the aim to facilitate and support fire protection work in European countries.

The market imposes new demands for quality and safety. Today fire protection forms an integral part of a modern strategy for survival and competitiveness.

The guideline is primarily intended for those responsible for safety in companies and organisations. It is also addressed to the rescue services, consultants, safety companies etc so that, in the course of their work, they may be able to help companies and organisations to increase the levels of fire safety.

The proposals within this guideline have been produced by VdS Schadenverhütung and the author is Hardy Rusch from Germany.

This guideline has been compiled by Guidelines Commission and adopted by all fire protection associations in the Confederation of Fire Protection Associations Europe.

Zurich, 27 April 2007
CFPA Europe

Dr. Hubert Rüegg
Chairman

Stockholm, 27 April 2007
Guidelines Commission

Tommy Arvidsson
Chairman

CFPAEUROPE

Contents

1 Introduction

Commercial and industrial plants, colleges and universities, as well as offices are highly dependent on the proper functioning of their information technology (IT) equipment. This equipment is of special importance due to the high demand on its availability and to its key role in production and administration processes. Failures of such equipment pose a serious threat to the company. Due to this special importance, most companies take loss prevention measures for IT equipment that go beyond legal requirements stipulated in building laws, occupational health and safety regulations etc. This guideline covers both equipment to be newly installed and existing equipment.

Note: An example checklist is included in Appendix 7.2. This is not meant to be exhaustive but gives a general survey and further notes on the individual loss prevention measures.

Protection measures should be appropriate to the risk and should define:

- the event which a protection measure aims to prevent;
- the way in which a measure shall be effective; and
- the extent of the loss that may occur.

The protection of IT equipment shall have high significance. An adequate safety level can only be guaranteed by an integrated concept. Special emphasis shall be placed on a sensible combination of protection measures. A main part of these measures is fire protection; any failure of the fire protection measures can lead to disastrous loss.

2 Scope

Within this guideline, IT equipment or facilities are data centres and server rooms, as well as central equipment used in the measurement and control of industrial processes, network engineering and communication. This guideline refers both to rooms and to technical equipment. If, due to local conditions, the loss prevention measures listed below and in the example checklist cannot be carried out in full, a choice of measures adjusted to the relevant conditions shall be taken.

National fire safety and prevention measures stipulated, for example by building authorities, industrial inspectorates and employers' liability insurance associations remain unaffected by this guideline.

3 Abbreviations

ITE	**I**nformation **T**echnology **E**quipment
IT	**I**nformation **T**echnology
FDFAS	Fire detection and fire alarm system
FES	Fire extinguishing system
SHEVS	Smoke and heat exhaust ventilation system

4 General risks in information technology facilities

Besides the risk of fire, smoke and explosions, the operation of an IT facility is subject to a lot of other different risks that may lead to damage to buildings, machines and to data loss. For example:

- failure of the power supply;
- overload (lightning strike, EMC, overtones, transient currents, etc.);
- faulty potential equalisation;
- water;
- intrusion, theft, vandalism and sabotage;
- natural perils (flood, storm, earthquake, etc.);
- faulty building design (selection of unsuitable rooms);
- faulty technical equipment;
- organisational faults (inappropriately skilled personnel);
- risks due to viruses, hackers, etc.

4.1 Global fire risks

Fire risks are present wherever combustible materials, oxygen and an ignition source coincide. As oxygen is available in all areas, the risk shall be assessed mainly on the basis of the amount of combustible material (fire load) and potential ignition sources. Unnecessary fire loads in areas containing IT equipment often favour a fast fire spread. IT equipment can be divided into several areas which should be assessed differently according to fire load and respective fire risk. A survey of the fire risks is given in Table 1.

Note: If an oxygen reduction system is used, please note that there is still a relevant oxygen content in the air of the protected area. This oxygen content is determined on the basis of the combustible materials in the protected area. And even for correctly designed oxygen reduction systems, smouldering fires and pyrolysis procedures are still possible.

Areas	**Risk due to**	
	fire load	**risk factors / ignition sources**
False floors, hollow screed	Relatively high fire load due to: • Power and data cables - cables that are no longer used - cables with flammable insulation made of halogen-containing plastics which have a damaging impact in the event of ignition due to corrosive smoke gases • Dust deposits	• Faulty contacts, loose connections and terminals • Small animals (rodents) • Technical faults in air-conditioning systems, emergency power supply, etc. can lead to inadmissible heating of equipment parts
IT room	• Fixtures (furniture, etc.) • Panelling and insulating material • Consumable and packaging material (paper) • Dust deposits	• Defective equipment • Negligence of personnel • Fire-hazardous works

Technical equipment (ITE, power distribution, climatic chambers, etc.)	• Plastics • Used equipment • Spare parts • Circuit boards	• Defective components • Overloaded power supply units • Missing or incorrect overload protection equipment • IT-incompatible electrical installations • Heat accumulation • Lightning strike

Table 1: Examples of fire risks

4.2 Fire risks from organisational faults

Typical examples of organisational faults, which can lead to a fire, are:

- inappropriate operation, lack or faulty maintenance of technical equipment;
- a lack of cleanliness and tidiness;
- a lack of consideration for fire-hazardous works;
- no control or briefing system for work conducted by external companies;
- no ban of smoking and open fires;
- insufficient training and briefing of personnel in relevant safe behaviour;
- misconduct during firefighting and other emergencies.

5 Preventive fire protection measures

Effective loss prevention for persons, goods and property can only be achieved by an overall concept adjusted to the individual company, offering an optimum combination of protection measures. Examples for such measures for the prevention of fire are listed in Table 2. Structural, system-relevant and organisational measures shall be coordinated so that the defined protection aims for the IT facility are achieved.

Structural, building and planning measures	System-relevant measures	Organisational measures
• Sufficient structural separation against fire • Protection of wire or duct penetrations against fire and smoke, with fireproofed bulkheads • Use of non-flammable materials • Sufficient static design of, for example, mountings etc.	• Fire detection and fire alarm system (FDFAS) • Fire extinguishing system (FES) • Smoke exhaust ventilation system (SHEV) • Wall hydrants/fire extinguishers • Protection against lightning and overload etc.	• Fire safety regulations • Fire brigade plan • Fire protection plan • Rescue route plan, operating instructions • Emergency signage/marking • Avoid unnecessary fire loads • Smoking ban • Permits: – fire-hazardous works – instruction of contractors • Training • Practices

Table 2: Protection measures

The measures which are taken should be written down in a document.

5.1 Structural fire separation

IT facilities shall be separated from adjacent areas by fire-resistant walls (of 90 minutes minimum resistance – REI/EI 90) and non-flammable materials.
Separating walls within IT facilities shall offer at least 30 minutes of fire resistance (REI/EI 30) and be made of non-flammable materials. They shall reach from the raw floor to the raw ceiling (also through false floors and false ceilings). IT equipment should possibly be distributed to several rooms.

IT areas shall not be located in the same fire zone as other high hazards, for example production or storage areas. High hazards shall be separated by fire break walls (walls with fire resistance of a minimum of 90 minutes – REI-M/EI-M 90) or complex separation walls (walls with fire resistance of a minimum of 180 minutes – REI-M/EI-M 180) with increased stability requirements in the case of fire and made of non-flammable materials. As a matter of principle, the insurer’s advice should additionally always be sought.

Any openings required in these walls (for example, doors, glazings, pipe and cable ducts, etc.) shall be designed according to the fire resistance class of the adjacent areas. Additionally, smoke spread shall be prevented efficiently.

Roofs above IT facilities shall not have any flammable roof covering or heat insulation.

5.2 Interior fittings

The interior fittings should be made of non-flammable materials; if this is not possible, at least materials of low flammability should be used as well as materials that do not drip while burning. As few halogen-containing plastics should be used as possible, both in IT facilities and in adjacent areas.

According to Table 1 unnecessary fire loads and potential ignition sources should be avoided in IT facilities.

5.3 Fire detection and fire alarm systems (FDAS)

IT facilities including adjacent rooms shall be monitored by automatic fire detection and fire alarm system (FDFAS). Apart from the IT facility area itself these could include:

- plant rooms of air-conditioning or venting systems;
- ventilation ducts from air-conditioning systems, including fresh air sampling pipes;
- rooms for power supply and emergency power supply;
- data archive rooms;
- paper storage rooms;
- rooms beside or above/below the IT facility.

False floors and rooms between false ceilings and storey ceilings shall also be monitored.

The FDAS shall fulfil the requirements of the European/national regulations and standards. In the majority of cases, smoke detectors are used for the monitoring of IT areas; the smoke detectors shall be appropriate for the area to be monitored and for the fire characteristics to be expected.

A so-called non-violent fire brigade access during fire alarm, e.g. via a key depot (also called a fire brigade key box) should be installed and agreed by the local fire brigade.

In air-conditioned IT areas, especially those with forced ventilated electrical/electronic equipment, early detection of fires by common point smoke detectors is extremely difficult or even impossible due to the forced ventilation and the "dilution" of the fire characteristics. In order to ensure consistent fire protection in such rooms, local fire detection for this equipment is required in addition to the room monitoring.

Unlike classical fire detection and alarm equipment, which would in this case reliably detect only a rather advanced fire development, local application of high sensitivity aspirating smoke detectors ensures an early and locally limited response. These can be adjusted to offer different alarm thresholds that can trigger a number of loss-reducing responses.

5.4 Fire extinguishing systems (FES)

For the entire protection of IT equipment, automatic fixed fire extinguishing systems can be recommended. Both gas extinguishing systems and water extinguishing systems are appropriate for IT equipment, as well as adjacent areas, such as storage areas, archives and offices. These fire extinguishing systems may be either total flooding systems or local application systems. Local application systems ensure selective protection of the respective device or equipment part.

Before a fire extinguishing system is triggered, the air-conditioning system should be disabled automatically.

Water extinguishing systems are mostly sprinkler systems, mainly appropriate for building protection and life safety. Due to a residual risk of unwanted water discharge resulting in consequential damage to sensitive equipment, pre-action dry-pipe systems (so-called pre-action systems) are usually chosen. Tolerating a remaining risk that IT equipment might be damaged, water mist extinguishing systems may also be used.

For application in IT areas, in false floors, etc. extinguishants with as little residue as possible are preferable. These should be non-corrosive and not electrically conductive. The following gas extinguishing systems meet these requirements:

- carbon dioxide (CO_2) fire extinguishing systems;
- inert gas extinguishing systems;
- systems with chemical extinguishants, etc.

Each of these extinguishing systems has advantages and disadvantages regarding this particular application. Therefore, the type of extinguishing system shall be determined in the planning phase, taking into consideration the protection aim after consultation with a competent planning officer or an approved installation firm, as well as the fire protection department of the insurer.

Furthermore, in IT rooms that are not, or hardly, accessed by persons, oxygen reduction systems may be used to protect them effectively against fire hazards. It is important to make sure that special basic requirements are fulfilled: on the one hand the performance of the oxygen reduction system depends e.g. on the integrity and ventilation conditions of the enclosure, and on the other hand, the health of any persons accessing these rooms shall be protected.

Fire detection, alarm, triggering respective pre-action (sprinklers) of a fire extinguishing system and its monitoring is generally done by a fire detection and fire alarm system approved for this purpose.

5.5 Fire extinguishers

Both, in the actual IT equipment rooms and in the adjacent rooms, a sufficient number of appropriate fire extinguishers shall be available.

Powder extinguishers represent a great risk for IT equipment and should not be installed in IT equipment rooms nor in adjacent rooms. Instead fire extinguishers containing water, or water with additives, such as foam shall be used in adjacent rooms. Within the IT facility CO_2 extinguishers are preferred.

5.6 Smoke and heat exhaust ventilation systems (SHEVS)

New concept developments of IT equipment should include the installation of smoke and heat exhaust ventilators (SHEVS). The aim is to avoid damage of the IT equipment caused by aggressive smoke gases and heat exposure. To assure the immediate removal of smoke and heat, mechanical systems are preferred. To ensure the success of the smoke and heat exhaust system, an individual risk analysis is necessary.

The installation and operation of SHEVS shall be arranged to take into consideration the other technical equipment (e.g. extinguishing systems, air-conditioning system), and agreed by a fire protection expert. For example, smoke and heat exhaust ventilators shall not open automatically in rooms protected by a gas extinguishing system; this and further important requirements are included, for example, in the CEA specifications for gas extinguishing systems.

SHEVS should have the following characteristics:

- the system should be planned and designed especially for IT facilities purposes;
- smoke exhaust ducts and valves going through ceilings and walls of defined fire resistance classes should be designed in accordance with the appropriate fire resistance class;
- smoke exhaust ducts should be made of non-flammable materials only;
- the smoke exhaust system should be designed such that smoke and hot gases can be dissipated immediately during the fire occurrence;
- make up air openings leading outdoors should be designed such that they are protected against a negative impact from outside.
-

5.7 Organisational fire protection

A fire protection concept showing the necessary organisational measurements shall be established and specified for the IT facility. The following items shall be considered:

- reduce fire load to the minimum;
- set up regulations for the behaviour in case of fire, and train staff;
- set up mounting and installation instructions;
- strictly do not allow fire-hazardous works; if necessary, a permit is required and fire protection regulations shall be followed;
- instruct and supervise contractors;
- keep and control cleanliness and tidiness permanently;
- eliminate ignition sources;
- smoking ban; if necessary, provide separate fire protected smoking zones;
- ban private electrical appliances

For further details see also appendix 7.1 “Advice to the contents of an internal fire safety regulations document (prototype)”.

All necessary fire protection measures shall be agreed by the insurer, with the internal representative for safety and health and fire protection and with the responsible public fire brigade. They shall be outlined in a fire protection documentation, where the structural, technical and organisational fire protection measurements are detailed. Fire protection plans shall be kept updated at all times. A fire brigade plan, showing the facilities for the fire brigade and equipment in and around the building shall be handed to the competent fire brigade.

Note: For further information on organisational fire protection see also CFPA-E Guideline No 1:2002 - Internal Fire Protection Control.

5.8 Further loss prevention measures

During a fire, damage to the respective IT equipment can generally be minimised by well-timed manual disconnection of the voltage supply. Manual emergency abort devices shall be protected against accidental operation and abuse.

If IT equipment rooms are air-conditioned, they shall have their own air-conditioning systems. The air-conditioning system should possibly be located in a fire-resistant (fire resistance of minimum 90 minutes, non-flammable components) separated room outside the IT facility. The air-conditioning system should be controlled by a fixed, non-battery-operated control unit.

6 Reference Publications

- CEA 4001 Fire Protection Systems - Specifications for Sprinkler Systems - Planning and Installation
- CEA 4007 Fire Protection Systems - Specifications for CO_2 Systems - Planning and Installation
- CEA 4045 Fire Protection Systems - Specifications for fire extinguishing systems using liquefied "halocarbon" gases - Planning and installation
- CEA 4008 Fire Protection Systems - Specifications for fire extinguishing systems using non-liquefied "inert" gases - Planning and installation

Source: www.cea.assur.org - Free downloads - CEA Fire/Theft Specifications

7 Appendix

7.1 Advice on the contents of an internal fire safety regulations document

- Combustible material

  The quantity of combustible material shall be minimised. Only essential paper documents shall be available and kept in sheet cabinets.

  If possible, flammable liquids shall be exchanged for non-flammable substances. They shall be kept in unbreakable, leak-proof containers.

  In IT facility rooms, the IT equipment shall not be stored in the packaging.

- Behaviour in the case of fire

  The staff responsible for taking special measures in the case of fire shall observe the respective instructions.

- Mounting and installation works

  During IT mounting and installation works, it is essential to keep the place clean and tidy, avoid any accumulations of combustible material, comply with the smoking ban and keep out any other ignition sources.

- Hot works

  Hot works shall be banned on principle. If they cannot be avoided in exceptional cases, special protection measures shall be taken. Hot works shall be authorised in writing. The authorisation shall specify the protection measures to be taken and name the responsible persons.

  Note: For further information relating to hot works see also CFPA-E Guideline No 12:2006 – Hot work safety.

- External firms
  The staff of external companies shall be instructed on any operational specifics and on the regulations to be kept in the case of fire; when placing the order, the external staff shall commit in writing to comply with the safety regulations.

- Cleanness and tidiness
  The entire IT facility shall be kept especially clean and tidy. Any waste shall be removed from the IT facility not later than at the end of any shift and shall be duly disposed of.
  Closed non-combustible waste containers with self-closing lids shall be used. If possible, they should be positioned outside the IT facility or in an area with fire protection separation.

- Ignition sources
  In the IT facility, open fires are strictly forbidden. This includes, of course, a smoking ban. Compliance is controlled, offences are prosecuted.

- Private electrical devices
  The use of private electrical devices in the IT facility rooms is not permitted for fire protection reasons. Exemptions shall be granted in writing following a safety inspection of the devices.

7.2 Check list example

	Yes	No	Not relevant
Tidiness and cleanliness in the IT facility/Organisation			
The IT facility is devoid of furniture and other objects.			
Waste and packaging materials are removed on a regular basis.			
The smoking ban is complied with.			
Fire drills have been carried out.			
No private electrical devices are available in the IT facility rooms.			
Electrical system/Lightning and overvoltage protection			
No combustible materials are stored near electrical distributors, switchgear or battery charging stations.			
Only authorised devices are in operation.			
Compulsory inspections of the lightning and overvoltage protection system have been carried out.			
Fire and smoke doors			
The doors are functional (closing device not wedged).			
Doors are freely accessible (not blocked, e.g. by stored goods)			
Openings in fire compartment walls and ceilings			
Have all cable and pipe ducts been sealed appropriately?			
Have ducts in the construction site area been sealed provisionally?			

Manual extinguishing equipment			
All fire extinguishers and wall hydrants are freely accessible.			
Fire extinguishers are inspected on a regular basis and positioned appropriately.			
Hot works			
The safety procedure for hot works has been applied at all times.			
Fire detection and fire extinguishing systems			
Regular maintenance and inspection works have been carried out.			
The systems are operational; e.g. no detectors have been disabled.			
Alarms / emergency calls			
The emergency call system is operational.			
The voice alarm system is operational.			
Intercoms (e.g. in lifts) can be used for emergency calls.			
Emergency organisation			
Emergency call lists and emergency plans are up to date.			
Emergency instructions for reception desks and plant protective forces/security guards are up to date.			

Carried out on: ....
Signature: ....
Forwarded on: ....

8 European guidelines

Guideline No 1:2002 - Internal fire protection control
Guideline No 2:2007 - Panic & emergency exit devices
Guideline No 3:2003 - Certification of thermographers
Guideline No 4:2003 - Introduction to qualitative fire risk assessment
Guideline No 5:2003 - Guidance signs, emergency lighting and general lighting
Guideline No 6:2004 - Fire safety in residential homes for the elderly
Guideline No 7:2005 - Safety distance between waste containers and buildings
Guideline No 8:2004 - Preventing arson – information to young people
Guideline No 9:2005 - Fire safety in restaurants
Guideline No 10:2007 - Smoke alarms in the home
Guideline No 11:2005 - Number of fire protection trained staff
Guideline No 12:2006 - Fire safety basics for hot work operatives
Guideline No 13:2006 - Fire protection documentation
Guideline No 14:2007 - Fire protection in information technology facilities
Guideline No 15:2007 - Fire safety in guest harbours and marinas