



A data centre is a facility used to house computer systems and associated components, such as telecommunications and data storage systems. They are processing an ever increasing quantity of videos, voice and data throughout a global network. Applications such as social media, cloud computing and online banking impact our life every day.

With the value of data being extraordinarily high, down time is not an option. Servers are packed together, the power is always on, they generate heat, and while not widely publicised, they do catch fire.

Assets surrounding the fire suffer collateral damage from water and smoke, with smoke contamination often destroying other nearby electronic equipment. The cost of business interruption, including software recovery and clean up is often significantly more than the cost of the asset destroyed in the fire.

All personnel working in the data centre should be trained on what to do in a fire-related emergency. It is also important to have a plan for any emergency situation. Run through fire drills, evacuation plans and recovery plans to keep everyone up to speed. Each person in the data centre must know how to operate a fire extinguisher. There should be a sign next to every extinguisher that clearly indicates what type of fire they can be used on.

**The high value and sensitivity of the electronic equipment found in modern data centres, combined with the consequences of system interruption, makes fire protection a critical component of any risk assessment.**

Fires can occur within the digital equipment, wires, cables, HVAC equipment, raised floors, suspended ceilings, and other combustibles found in data centres. Uninterrupted power systems and their storage batteries pose an additional fire risk.

These fire risks lead data centres to address fire protection at three different levels – building level, room level, and a rack-level (in-cabinet).

### **Building Level Fire Protection**

The first level of fire protection is at the building level. The main goal is to protect the building and employees from fire. The type of fire protection most commonly used is fire sprinklers and handheld extinguishers. A building can also use passive fire protection, which is the installation of firewalls and fire-rated floor assemblies that considerably delay the spread of fire into other areas of the building.

### **Room Level Fire Protection**

A wet pipe sprinkler system has the water already present in the piping and can immediately disperse once the alarm activates. The downside to this type of sprinkler system is the pipe can leak and drip onto equipment in the room. A pre-action system is the most commonly used for room fire protection. It requires at least two points of fire detection to activate the sprinkler system. However, water can cause as much damage to servers and hard drives as a fire would.

Many data centres prefer gas extinguishing systems. Clean agent gas systems have a smaller footprint than inert gas systems because they do not require as much agent to fill up an entire room. Clean agent gases are electrically non-conductive, non-corrosive, and leave no residue upon evaporation. This makes them the ideal fire suppression agents in data centres. Like fire sprinklers, these systems have a piping system installed throughout the room. The system activates through smoke and heat detection, and the clean agent gas disperses evenly throughout the room through nozzles.

### **Rack Level Fire Protection**

The last level of data centre fire protection is at the rack level. This fire protection is essential to protecting specific equipment and limiting damage. Installing a pre-engineered automatic fire suppression system will protect the equipment by detecting the fire within seconds and suppress it before the total flood or sprinkler system activates. This prevents equipment damage caused by a water-based sprinkler system and avoids the discharge of large amounts of agent in a total flood cylinder which is expensive to refill.