

Data Centres – Cooling and Ventilation

Data centres contain highly sensitive equipment and systems with specific temperature, humidity and other environmental requirements. Incidents involving cooling and ventilation equipment can cause significant damage to data centres leading to downtime and business interruption losses.

Guidance on preventing such incidents, and mitigating the extent of damage, are discussed in this Loss Prevention Standard.

Data Centres –Cooling and Ventilation

Introduction

Data centres house computer hardware and ancillary equipment for the processing, management, and storage of data, and other related systems including telecommunications.

This equipment utilises large amounts of electrical energy and generates significant heat outputs. The sensitivity of the equipment to environmental conditions means that effective cooling and ventilation are critical in managing the facility and reducing the risks of damage or loss.



This is one in a series of Loss Prevention Standards that provide risk management guidance in respect of data centres. This document provides an overview of the main cooling and ventilation systems in data centres with guidance on reducing the potential for loss or damage. Other standards in this series are detailed later in this document.

Note: This document relates to data centres. It is not for on-site data processing and storage facilities, typically provided within a business premises to support other trading activities. Please refer to the Aviva Loss Prevention Standard Server/Comms Rooms for further guidance on such facilities. This document focusses on Property loss prevention and related risk management guidance and is not intended to address Business Interruption or Liability exposures. The presumption is that all regulatory requirements, such as Fire Risk Assessments, have been met.

Understanding the Risks

A number of risks and hazards are associated with the cooling and ventilation systems in data centres. These include but are not limited to:

- **Overheating.** Poorly designed, underspecified or faulty cooling and ventilation systems can lead to overheating and associated breakdown or fire events.
- **Smoke Contamination.** Poorly designed cooling and ventilation systems can spread smoke from a small fire in a non-business critical building area into a data hall, or from one data hall into adjacent data halls.
- **Condensate.** Condensate from drain lines can leak, causing an escape of water event.
- **Contamination.** Damaged or compromised ventilation systems and filtration can allow airborne contaminants into the data halls, which can damage sensitive components.
- **Leakage.** The water and other liquids used in cooling, or fire protection systems can leak and damage equipment.

- **Humidity.** Atmospheric water levels need to remain constant and within specified parameters. High or low humidity conditions can lead to electrostatic discharges or increased condensation and corrosion issues.
- **Condensation.** The combination of air temperature, air humidity and surface temperature of ‘cold surfaces’ can give rise to condensation and therefore a water exposures.
- **Performance.** Optimised heating and cooling systems can aid the performance and longevity of data centre equipment and components.

Cooling and Ventilation Systems

Data centres generate significant amounts of heat and require intelligent cooling, ventilation, and humidity control systems to maintain optimal server performance and reduce the potential for damage to servers and associated equipment.

The requirements of the cooling and ventilation systems are dictated by a number of factors in the design including:

- The location of the data centre geographically. Local humidity and temperature fluctuations will have a direct impact.
- Equipment manufacturers recommended operating temperature and humidity guidelines. This will be driven by equipment type and the different vulnerabilities of the equipment in use.
- Data hall configurations, layout and rack orientation, equipment density and separation distances between racks, etc.
- The building performance for issues such as heat absorption and emissions, moisture ingress, etc.
- Future proofing the design for possible increase in server rack numbers.
- Fluctuations in processing power usage. This can significantly impact the heat generated at any given time. As such, cooling systems must be able to adapt swiftly to maintain the optimum temperatures.

Note: It is critical that humidity levels are maintained at the thresholds specified in the design specification and operating guidelines. Humidity levels that are too low can lead to electrostatic discharge, whilst high humidity can lead to condensation build up and the associated corrosion and potential for shorting.

Air Cooling

Most data centres utilise air cooling technology. The systems work by removing heat from the circulating air and replacing with cooler air. This is typically done in one of two ways:

1. Removing/extracting hot air from the data hall and replacing it with fresh air drawn into the hall. This is then cooled (unless already sufficiently cold) and circulated through the data hall.
2. Recycling air within the data hall itself, and cooling, typically via a ‘hot and cold aisle’ system.

The most common methods of air cooling are:

Computer Room Air Conditioners (CRAC). These systems have a low cooling capacity and are typically found in older and/or smaller data centres. These systems use traditional ‘expansion based’ refrigerant cooling via internally located evaporators and external condensers.

Delivery can be via overhead ducting, independent wall or ceiling units or raised floor systems which deliver cold air through the ducting within the data hall floor displacing the warmed air where it is either removed or recycled for cooling and recirculation.

Computer Room Air Handlers (CRAH). These systems have a high cooling capacity and are commonly used in large and high-density data centres. Delivery is typically via raised floor systems.

Hot and Cold Aisle. To aid efficiency of air-cooling systems, server cabinets are typically configured into hot and cold aisle arrangements. The cabinet rows face each other in opposite directions so that cold intake and hot air ventilation create alternating aisles of cold and hot air, enabling hot air to be vented via the hot aisle and cold air delivered in the cold aisle.

Evaporative Cooling

Evaporative cooling is a method of cooling air without the use of refrigerants. The system works by passing air across wet filter pads, where the evaporation process cools the air and is then ducted around the data hall. Heat exchangers may be employed in more complex systems to isolate the cooling process from the air delivered into the data hall.

Evaporative cooling is most commonly used in warm and dry environments with low relative humidity and is a very energy efficient and environmentally friendly method of cooling.

Other Cooling Types

Other cooling systems are available including:

- Liquid cooling and immersion systems, which are becoming more popular in Artificial Intelligence (AI) led centres.
- Hybrid liquid and air systems
- Geothermal cooling which uses the natural cool temperatures of the earth's substrata to cool agents within closed loop systems
- Solar cooling.

All of which are relatively new technologies and outside of the scope of this document.

Monitoring Systems

Environmental monitoring systems are essential in managing the cooling processes and reducing the risks of breakdown, leaks, overheating and other damage. These need to be reliably connected to a delivery platform that is monitored by appropriately trained personnel to respond as needed. Monitoring should include at least the following:

- **Air Temperature.** Temperature probes should be present throughout the server racks and hall at varying heights to ensure the most accurate monitoring.
- **Coolant Flow and Return Temperatures.** Ensures unusual low flow rates or high temperatures within the coolant cycle are identified for rectification.
- **Differential Air Pressure Monitoring.** Poor air pressures and air flow within server racks can reduce cooling efficiency, typically as a result of poor containment, e.g., missing or poorly fitted panels.
- **Humidity Monitoring.** Helps avoid excessive condensation, corrosion, electrical shorting and mould accumulation, all of which can lead to damage or loss.

- **Electrical Current Monitoring.** Power related faults can cause disproportionate levels of damage and outage. Continuously tracking and analysing the flow of electrical current to the various components and systems within the data centre can help reduce the potential for such damage. Monitoring should include real time monitoring, residual current leaks and load balancing.
- **Leak Monitoring.** Condensate can occur due to excessive humidity or water ingress and/or escape of water or cooling fluids can occur where they are present. Water or liquid leakage sensors are essential in detecting such issues and should extend to all areas of the data hall including concealed floor and ceiling voids/plenums.

Monitoring systems should be subject to maintenance, checks and calibration as per Original Equipment Manufacturers (OEM) or installer guidelines.

Important: Any false ceilings or screens installed to reduce room height and improve the efficiency of cooling systems, should be non-combustible and should not obstruct or impair fire detection or fire protection systems.

Managing the Risks

- The systems should be designed specifically for the server and other IT equipment within the data halls based on the planned equipment.
 - ✓ Ensure the systems reflect any future growth plans.
 - ✓ This helps avoid expensive downtime for infrastructure upgrades.
- The systems should be designed and the cooling requirements, calculated by a competent person or company.
 - ✓ Systems should be designed specifically for the data hall environments and the estimated heat output/electrical current draw.
 - ✓ It also needs to include expected maximum summer temperatures. This is particularly important when considering fresh air arrangements.
- Redundancy/back-up arrangements should be designed to provide sufficient back-up capability that can take over immediately should the primary system fail.
 - ✓ Fully mirrored systems with independent power and distribution systems are recommended, if warranted by the business exposure.
 - ✓ Ensure this extends to monitoring systems.
- Ensure the systems can accommodate reasonable changes to data hall layout and additional equipment.
- Any filters used in the cooling and ventilation equipment should be non-combustible.
 - ✓ Filters should be replaced on a frequency to prevent them from being laden with combustible dusts that can then present a contamination risk or an additional fire load.
 - ✓ Spare filter media should be stored in a separate dedicated fire compartmented storeroom and not within the data hall.
- All cooling and ventilation equipment, including monitoring systems should be subject to maintenance, self-inspection checks and calibration as per Original Equipment Manufacturers (OEM) or installer guidelines.
 - ✓ Use thermographic cameras to help detect unusual heat patterns, such as hot and cold spots.

- The systems designer and the installers of any detection and fire protections should liaise to ensure the air movements within the data processing/storage facilities do not impact performance of the fire systems.
 - ✓ The velocity of air within the data hall; stagnant air pockets or ‘dead air’ spaces e.g., corners of the hall, thermal convection currents, etc. all need to be carefully considered when looking at ‘air movement’ and the fire detection and fire protection strategy of the data hall.
 - ✓ On many occasions air stratification, air velocity and stagnant air pockets in data halls have compromised installed fire detection and fire suppression actuation mechanisms.
 - ✓ The air ventilation and cooling systems need to be able to allow a ‘lazy smoky’ fire to actuate and alarm the fire detection system within the data hall.
- Any changes to the layout of the data halls, additional server equipment, etc., should result in the cooling and ventilation provision being reviewed for adequacy and stepped up where necessary.
 - ✓ A formal change management process should be adopted for this and any other significant planned or emergency changes.
- Ensure emergency response planning to system faults and issues has been documented and appropriate training provided to appropriate employees.

Fire and Smoke Resilience

Fresh air, recirculating air and exhausted air associated with a data hall must not compromise the fire and smoke resilience arrangements. The design of the cooling and ventilation systems should be based on the business exposure and the potential impact from a smoky fire. As a result:

- The ventilation and cooling system design should not compromise any fire and smoke compartmentation strategy.
- The ventilation system should be designed with the understanding that heat and smoke venting from a fire is either designed into the system or a dedicated heat and smoke venting system is designed separately.
- Ventilation exhaust areas should not be positioned where exhausted air can be drawn into an adjacent fresh air intake.
- Ventilation equipment for one data hall should not be housed in the same plant room as that for another data hall. In this case, one fire could impact all ventilation equipment.
- Cooling and ventilation systems from non-data hall ancillary areas and data hall areas should not be manifolded. They should remain separate. This includes for any utility rooms and uninterruptable power supply (UPS) rooms.
- Cooling and ventilation systems from one data hall and another data hall should not be manifolded. Each data hall should have its own dedicated arrangement.
- The ability to clean the ventilation ducting should be considered in the system design, especially for those systems used for heat and smoke venting, post a fire event.
- The type and location of any fire detection or suppression systems, together with any accompanying interlocks, should be considered as a part of a coherent fire/smoke resilient and cooling/ventilation arrangement. This could include the provision of automatic fire detection:
 - ✓ Within the cooling and ventilation system.
 - ✓ Across any fresh air in-take.
 - ✓ Across any air recirculation interfaces.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

- Leak detection and prevention - [LeakSAFE](#)
- Leak detection and prevention - [Ouensus](#)
- Thermal Imaging Cameras and PAT Testing Equipment - [Pass](#)

For more information please visit: [Aviva Risk Management Solutions - Specialist Partners](#)

Sources and Useful Links

- [Risk Management Guides | Aviva Risk Management Solutions - Aviva Risk Management Solutions](#)
- [Insurer Requirements for Enhanced Escape of Water Protection Based on Approved Document G of the UK Buildings Regulations](#)

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Data Centres - Planning and Design**
- **Data Centres - Construction**
- **Data Centres - Detection and Fire Protection**
- **Data Centres - Escape of Water and Other Fluids**
- **Data Centres - Fire and Smoke Resilience**
- **Escape of Water and Other Fluids**
- **Escape of Water on Construction Sites**
- **Escape of Water - Installation and Maintenance**
- **Escape of Water - 10 Top Tips**
- **Escape of Water - Responding to Incidents**
- **Work on Wet Systems**
- **Self-Inspections**
- **Maintenance Regimes**
- **Managing Contractors - Property**
- **Sprinkler Systems Winter Precautions**

To find out more, please visit [Aviva Risk Management Solutions](#) or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

26th March 2026

Version 1.0

ARMSGI3792026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.