Data Centres – Planning and Design

Incorrectly designed and built data centres can generate significant risks. Hazards such as fire, smoke, water ingress, and other environmental or structural threats can severely impact critical infrastructure. It is therefore essential that data centres are developed with a robust, integrated design approach that prioritises resilience, and can accommodate future business needs.

This Loss Prevention Standard provides an overview of the main data centre planning and design considerations.

Version: 1.1
Date: 26th March 2026

Data Centres – Planning and Design

Introduction

Data centres are used for the housing of critical computer hardware and ancillary equipment for the processing, management, and storage of data, and other related systems and applications including telecommunications.

Whilst major property damage events within data facilities are uncommon, the consequences of even the most minor of incidents can be significant, including fire and smoke damage or contamination to buildings and equipment, business interruption losses for service users and impacts on environmental, sustainability and governance objectives.

This is one in a series of Loss Prevention Standards which provide risk management guidance in respect of data centres. This document provides an overview of the main activities, management controls, critical processes, and equipment within most data centres, along with design recommendations to help improve the resilience of the building and its infrastructure. Other standards in this series are detailed later in this document.

Note: This document relates to data centres. It is not intended for on-site data processing and storage facilities, typically provided within 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.

Background

Types of Data Centre

Data centres can be either managed in house, whether at individual sites or at centralised locations, or outsourced to third party providers. Types include, but are not limited to:

- **Co-location Data Centres**. Standalone data facilities, typically owned and operated by third-party suppliers providing space and IT infrastructure but allowing organisations to use their own hardware.
- **Managed Services Data Centres**. Managed services data centres are owned and operated by third-party suppliers to provide full data management support.
- **Large-scale Data Centres**. Very large facilities used by the main technology companies to support rapid cloud-based service to individuals and organisations.

Other cloud-based centres are also available providing on-demand access to computing resources, storage, and applications over the internet.

Data Centre Equipment

The equipment found in data centres commonly comprises:

Server Racks. Servers process, store, administer and manage data. Data centres typically feature large halls, with extensive arrays of servers within cabinet racking.

Network Infrastructure. The network system connects server equipment used for processing and storing data within the centre and also to other connected data centre facilities as well as end-user locations.

Power Supplies. Data centres require significant power supplies, and this is expected to increase with artificial intelligence (AI) driven advancements. The energy required to operate a data centre facility often exceeds the available public supply and some facilities will incorporate large scale high voltage transformer equipment and on-site power generation such as that provided by gas turbine power plant, combined heat and power (CHP) co-generation, renewable energy systems, e.g., roof or ground based solar photovoltaic, wind turbines, etc. In addition, extensive back-up power supplies are required to cover utility outages, instability, etc. These include back-up generator plant, battery energy storage systems, uninterrupted power supplies (UPS) and localised battery backup systems, often located within server racks.

Cooling and Ventilation Systems. Server equipment generates significant heat which needs to be removed from the facility and replaced or blended with cool incoming air to maintain constant temperatures. The cooling system capability and performance are critical to the management of a data centre.

Other Systems. Electrical installations, telecommunications, security hardware, detection and fire protection systems, etc.

Planning and Design Considerations

Consideration to the design and layout of the facility is essential in reducing loss potential.

Flood Exposures

Data centres should not be located in an area vulnerable to flooding. Even where the building is built above anticipated flood levels, foul water can still enter the building via drainage and sump systems during flood events.

- A flood risk assessment should be completed and appropriate flood resilience measures implemented and maintained, such as non-return/backwater valves to basement and ground level drainage systems, proprietary flood barriers, relocation of electrical services to elevated positions, upper floors, etc.
- Where flood potential has been identified, a formal Flood Emergency Response Plan should be produced (this may form part of your overall Business Continuity Plan), which will detail how the business will respond to the threat of flooding.
- Aviva Loss Prevention Standards **Flood Guidance and Mitigation Global, UK Flood Guidance and Mitigation and Flood - Emergency Response Plan** provide guidance on undertaking risk assessments, implementing flood resilience measures and emergence response arrangements.
- The Code of Practice for Property Flood Resilience produced by CIRIA (Construction Industry Research and Information Association) provides useful, practical guidance on managing flood exposures.
- Aviva Specialist Partner Apex Flood Solutions can assist with flood mitigation planning and protection.

Exposure

An assessment of any risks presented by other buildings or occupancies in proximity to the data centre should be undertaken as part of the planning phase. This also includes car parking and external storage areas, where the exposure presented may fluctuate.

- This can help identify hazardous exposures in the area that could present an increased risk of fire or contamination in the event of a fire incident.
- Contingency and emergency planning arrangements may need to reflect any local risks or concerns.

Refer to Aviva Loss Prevention Standard **Third Party Property Exposures** for further guidance.

Fire and Smoke Resilience

Guidance of fire and smoke compartmentation and resilience can be found in the Aviva Loss Prevention Standard **Data Centres - Fire and Smoke Resilience**.

Water/Fluid Risk Controls

Guidance on the management of water and other liquid related hazards can be found in the Aviva Loss Prevention Standards **Data Centres - Escape of Water and Other Fluids**.

Cooling and Ventilation

Date centres require intelligent cooling, ventilation, and humidity systems to maximise system performance and reduce the potential for damage to sensitive server equipment.

Specific guidance on these systems can be found in the Aviva Loss Prevention Standard **Data Centres - Cooling and Ventilation**.

Efficiency

Stressing the hardware used in data centres can contribute to increased likelihood of equipment breakdown, longevity issues and performance concerns. Increasing the capacity of data equipment and servers, etc., thereby reducing the operating requirements of each component in the system can reduce the potential for such issues, as well as reducing maintenance, repair, and cooling costs. This should be factored into the system design.

Redundancy

Data centre facilities should be designed to provide sufficient back-up arrangements that can take over immediately in the event of failure of any primary system(s). This can help reduce the impact of outages, ensuring that services remain available, and downtime is minimised. There are two redundancy strategies normally considered within data centre facilities:

- **2N** – Refers to a fully mirrored system with independent power and distribution systems. If one system fails, the mirrored system should immediately activate and limit any potential downtime. This is generally considered the most robust redundancy strategy with the highest fault tolerance however requires significant cost to establish, operate and maintain.
- **N+1** - If N equals the capacity needed to run the facility, N+1 indicates an additional component added to support a single failure or cover downtime for maintenance. This is generally considered a simpler and more cost-effective redundancy strategy and is typically employed for supporting systems such as UPS, monitoring, generators, or generator start-up equipment, etc.

It is important to include other associated systems such as heating, cooling, air handling, fire protection, etc., when considering redundancy arrangements. Conducting a risk assessment can help identify such systems, their potential vulnerabilities or those where single points of failure exist. These risks should be prioritized, based on their potential impact, and redundancy management strategies developed to mitigate their potential to cause downtime, loss or damage.

Important: When considering the 2N or N+1 philosophies, or other resilience strategies (e.g. N+2), it is critical not to locate the primary system and the redundant or back up system in the same fire or smoke compartment. A single incident could expose and compromise both provisions e.g., fire.

Important: When considering cabling or piping networks, any resilience in the provision should be diversely routed i.e., different directions; separate trunking, etc.

It is critical to identify single points of failure and establish a strategy to mitigate or prevent that exposure from being realised.

Electrical Hazards

The electrical systems installed at the location should be designed, installed, and maintained in accordance with national regulations, codes, or standards.

High voltage electrical works (exceeding 1kV) should only be designed, installed, commissioned and maintained by companies and personnel with appropriate qualifications, experience and competency, preferably as a full/complete delivery offering.

- Accreditation to installer schemes such as the National Electricity Registration Scheme (NERS) in the United Kingdom is essential when working with national distribution networks.
- Ensure the provider has sufficient authorised persons (AP); qualified and trained persons, operating and overseeing the installation works.
- All works should be based on risk assessment and method statements (RAMS) and be installed in compliance with key legislation.

Low voltage electrical works (below 1kV) in the United Kingdom should comply with **BS 7671:2018+A3:2024 - Requirements for Electrical Installations. IET Wiring Regulations**.

- The work to be carried out by competent, qualified contractors who are preferably a member of appropriate UKAS (United Kingdom Accreditation Service) installers and/or inspectors schemes.
- Ensure the electrical system design capacity reflects future growth plans.

Refer to the Aviva Loss Prevention Standard **Electrical Installations - Inspection and Testing** for further guidance.

Cabling

Most cabling will feature polymer insulation which can be combustible and produce harmful smoke in a fire event. To help reduce the potential for cable related fire damage, fire resistant cabling should be used wherever possible (plenum rated cabling). In addition, the cable arrangements and routing should be carefully reviewed to minimise the exposure to the data centre.

- Consider diverse and multiple routes for the cabling.
- Establish what fire loads could be located exposing internal and external cabling.
- Establish if any escape of water incidents could expose the cabling. Can the cabling be located in a way to reduce this e.g., raised from the floor by 100mm in a 300mm deep floor void.
- Power and data cables should be segregated and housed in separate dedicated cable trays or trunking.
- All cabling should be secured to the cable trays. This includes horizontal and vertical runs.
- Cable trays stacked vertically above each other should be avoided. The fire load and business exposure increases significantly with vertical stacks.
- Implement a cable management plan.
  - ✓ This includes organizing cables neatly, conducting regular inspections, and timely replacement of damaged cables.
  - ✓ Cabling should be minimized in floor and ceiling voids
- Following any works, all redundant and legacy cabling should be removed, and any openings fire-stopped to the same fire resistance rating as the fire compartment penetrated.

Refer to the Aviva Loss Prevention Standard **Data Cabling** for further guidance.

Lighting

Ensure lighting system design excludes the use of high-powered lighting such as High Intensity Discharge (HID) and halogen lighting.

- Light Emitting Diode (LED) lighting is preferred due to the reduced ignition hazards.

Refer to the Aviva Loss Prevention Standard **Electrical Lighting - Property** for further guidance.

Battery Backup Systems (BBUs) and Uninterrupted Power Supplies (UPS)

Power outage is a significant risk exposure that requires careful management and appropriate back-up systems to help mitigate any consequences.

To assess the back-up needs, power loads within the data centre should be grouped into

- **Critical**. e.g., servers, cooling systems and monitoring systems, etc.
- **Essential**. e.g., lighting, fire/security protections, etc.
- **Non-essential loads**. e.g., those loads that can drop out without compromising data centre operations.

Non-essential, and some essential loads will typically drop out until back-up generator equipment activates. Some essential loads may be connected to UPS, e.g., emergency escape signage, etc., whereas critical loads will typically be connected to either or both BBUs and UPS. BBUs provide instant power response to small, momentary power fluctuations and interruptions and are often located within server racks in proximity to the servers they support, whilst UPS provide protection from short term power outages prior to generator equipment taking over the power demand.

The batteries used in BBUs and UPS are typically lithium-ion battery technology, which whilst acknowledged as generally safe can on occasion enter thermal runaway, overheat, emit flammable and contaminating gases and ignite, usually when damaged, faulty or as a result of charging issues, etc.

To help minimise the effects of such an incident:

- UPS equipment should not be housed within the data halls. UPS equipment should only be installed within a separate room or compartment remote from the data hall environments.
  - ✓ The fire resistance rating (insulation and integrity) should be at least 2 hours.
  - ✓ The safe management of smoke and gas emissions resulting from both BBU and UPS lithium-ion battery fires and off-gassing events should be risk assessed. Additional mechanical ventilation should be installed, suitable for use in the atmospheres expected. This ventilation system should not be manifolded to any ventilation system associated with the data hall itself.

  Refer to the **Aviva Loss Prevention Standards Data Centres - Fire and Smoke Resilience** and **Data Centres - Cooling and Ventilation** for further guidance.
- The number of BBUs in server racks should be minimised as far as achievable and positioned to enhance ventilation and maintain full coverage by fire detection and protection systems.
- The batteries in both BBU and UPS systems will need to be monitored for charging and general performance, health, etc., preferably via sensors to each battery within the BBU and UPS systems.
  - ✓ Batteries should be replaced prior to lifecycle charging thresholds and immediately if dropped, faulty or monitoring systems and/or operators have identified any performance concerns including unusual odours, swelling, heat, etc.
  - ✓ Response arrangements should be formalised for faults or alarms.
  - ✓ Thermographic cameras should be used to check for hot spots or other unusual heat patterns.
- Ensure monitoring systems will be subject to maintenance, checks and calibration as per Original Equipment Manufacturers (OEM) or installer guidelines.

Refer to the Aviva Loss Prevention Standards **Lithium-ion Batteries - General Considerations** and **Use of Thermographic Cameras - General Considerations** for further guidance.

Standby Generators

Standby generators are configured to automatically start in the event of power failure and supply power to key equipment within the data centre.

- The generator(s) should be suitably sized to power all critical and essential loads within the data centre. This should include an assessment of future needs and this be considered in the initial design.
- Control systems should provide rapid synchronisation to ensure full power load is achieved promptly.
- Generators should be located 10 metres from the data centre and not in proximity to air intake systems.
  - ✓ If 10m separation is not possible, generators should be, at a minimum, located within dedicated fire compartments with at least 2 hours fire resistance rating (insulation and integrity). These to be located in an area that would be accessible in an emergency situation.
  - ✓ Exhaust discharge points should be located so that exhaust fumes cannot be drawn into any air inlets, so potentially contaminating sensitive components.
  - ✓ Exhaust lines and manifolds should be lagged with non-combustible materials.

- Main fuel tanks (excluding integrated 'day tanks') should be at least 10 metres from the data centre.
  - ✓ Bunding should be installed to provide at least 110% of total storage capacity.
    - Ensure any diesel storage complies with local or national pollution regulations, such as the **Control of Pollution (Oil Storage) Regulations** in the United Kingdom.
  - ✓ Fuel tanks and associated pipework, bunding, etc., should be protected against the risks of impact from vehicles, machinery, etc.
  - ✓ Ensure appropriate earthing protection is in place, where required.
  - ✓ A flame arrestor should be provided if a breather vent is provided for the fuel tank.
- Each data centre should have its own dedicated standby generator capability with adequate back up provision.
- Generator equipment should be subject to regular formal maintenance by suitably trained persons in accordance with OEM or accepted best practice guidelines.
- Generators and associated fuel storage should be provided with appropriate automatic fire detection, fire suppression and interlocks to shut down the fuel supplies, shut down the engine in a fire scenario.

Roof Mounted - Solar Photovoltaic (PV) Installations

Solar PV systems are often installed on data centre buildings to support energy demand. Fires involving roof mounted solar PV systems are not uncommon, and key considerations include:

- Ensure experienced and competent designers/installers are utilised.
- Do not install Solar PV systems on combustible roof materials, this includes composite or built-up systems with combustible insulation.
- Locate inverters, isolators, switchgear, etc., on well-ventilated, non-combustible surfaces. Where equipment is installed internally, locate within a fire rated compartment.
  - ✓ At least 2 hours fire resistance (insulation and integrity).
  - ✓ Ensure adequate ventilation is provided.
- Ensure solar PV panel framing is secured to the building, rather than ballasted frame mountings, which can be less resilient to adverse weather.
- Solar PV installations should be fitted with voltage optimisers which increase energy yield and automatically reduce the voltage within faulty panels to safe levels, reducing the potential for fire events.
- Create a number of separate roof arrays with at least 1 metre's separation. This acts as a fire break.
- Install skirting around the underside of the solar PV panels to help prevent combustible waste accumulating and deter nesting birds.
- Regularly inspect the installation for damage, faults and shading (which can lead to internal damage, shorting and possible ignition).
- Ensure a formal maintenance plan is in place with an experienced and competent company.
  - ✓ Aviva Specialist Partner Solarsense can assist with maintenance needs.

The following Aviva Loss Prevention Standards provide useful guidance in managing Solar PV systems:

- **Roof Mounted Photovoltaic Solar Panel Systems - General Considerations**
- **Roof Mounted Photovoltaic Solar Panel Systems - Planning for Installation**
- **Roof Mounted Photovoltaic Solar Panel Systems - Installation and Construction**
- **Roof Mounted Photovoltaic Solar Panel Systems - Installed and Ongoing Care**
- **15 Top Tips for Roof Mounted Photovoltaic Solar Panel Systems**

Battery Energy Storage Systems (BESS)

BESS are used to capture and store energy, whether electrical power purchased from the grid at lower demands for later use, or from renewable energy sources such as roof mounted solar PV systems.

Whilst proprietary BESS, installed and maintained in accordance with manufacturers' guidelines and national or local regulations, standards or codes are generally safe and reliable to use, the risks, which include fire and explosion, need to be carefully managed including siting units at least 10 metres from buildings and other valuable assets, interlocked gas detection, etc.

Important: BESS should not be installed within data centre buildings.

The following Aviva Loss Prevention Standards provide useful BESS guidance.

- **Grid-Scale Battery Energy Storage Systems - Construction**
- **Grid Scale Battery Energy Storage Systems - General Considerations**
- **Grid-Scale Battery Energy Storage Systems - Ongoing Care**
- **Small Scale Battery Energy Storage Systems**
- **Planning a Battery Energy Storage System - 12 Top Tips**

Lightning Protection

Data centre buildings and the electronic equipment including monitoring and communications systems therein, should be protected against the risks of lightning damage including surge and transient surge.

- A lightning risk assessment should be completed by a competent person or company, preferably a member of a recognised quality scheme or body such as the Association of Technical Lightning and Access Specialists (ATLAS) in the United Kingdom.
  - ✓ Any lightning protection systems should be installed in accordance with relevant standards, such as **BS EN 62305 Pts 1 to 4 - Protection Against Lightning** to determine the direct and secondary effects protection needs of the building and vulnerable equipment.
- Any lightning protection should be subject to routine inspections of conductors, bonds, joints, electrodes and to ensure that any recently added services have been bonded as required.
- The lightning protection should also be subject to formal maintenance in line with OEM recommendations by an accredited company at least every 12 months.
- Lightning protection may be required to ancillary equipment such as generators and fuel supplies.

Refer to the Aviva Loss Prevention Standard **Lightning Protection** for further guidance.

Vehicle Charging

Vehicle charging equipment should be located remote from data centre buildings and other valuable assets, e.g., sprinkler tanks, generators, transformers. It should also be located in an area away from any building air inlets. At least 10 metres is recommended.

- The potential for fire spread is reduced where satisfactory separation between vehicles under charge and infrastructure is maintained.
- The combustion products can also be highly damaging to sensitive server and IT equipment should they access the data halls via ventilation systems.

Refer to Aviva Loss Prevention Standards **12 Top Tips for Electric Vehicle Chargers** and **Electric and Hybrid Vehicle Charging** for further guidance.

Detection and Fire Protection

Detection and fire protection systems should be installed within data centre buildings and other ancillary buildings. Detailed guidance can be found in the Aviva Loss Prevention Standard **Data Centres - Detection and Fire Protection**.

Important: All plans to install automatic detection and fire protection systems should be reviewed and accepted by your property insurer and broker.

Security

The security protections should be based on the findings of security risk assessments and include:

- Good quality perimeter protection, e.g., site fencing and secured vehicle and pedestrian gates.
- Authorised access control to the data centre building and all data halls, control rooms, UPS rooms, energy centres/plant rooms, including systems to remove authorisation immediately upon persons leaving the business, or who are no longer authorised to access the facility.
- Access for security personnel, should an emergency occur when data centre workers are not available.
- Monitored Video Surveillance Systems (VSS).
- Monitored Intruder and hold-up alarm provision.
- Cyber security arrangements.
- An appropriate level of response based on the nature of the security event.

Please refer to the following Aviva Loss Prevention Standards for further guidance:

- **Security - Computer Equipment**
- **Security - Doors and Windows**
- **Intruder Alarms - General Guidance**
- **Security - An Introduction to Closed Circuit Television (CCTV) Systems**
- **Cyber Security: Top 12 Tips to Protect Against a Cyber Attack**
- **Cyber Security: Ransomware**

Smoking

Ensure non-combustible smoking shelters are provided and located at least 10 metres from data centre buildings and other valuable assets.

Refer to the Aviva Loss Prevention Standard **Smoking and the Workplace** for further guidance.

Waste Arrangements

Waste storage presents a number of fire exposures, including deliberate and accidental ignition, and should be closely managed.

Secured, non-combustible, external waste compounds should be installed on solid hard standing surfaces and located at least 10 metres from data centre buildings, other valuable assets, and at least 2 metres from boundary fences. Where waste storage is within 2 metres of a boundary fence, consider the potential for deliberate fire starting and ensure the facing compound walls, extending at least 3 metres on each side, cannot be breached by ignited materials, e.g., solid panels.

Waste facilities within the data centre buildings should be minimised and limited to non-critical areas only, such as rests rooms and general offices. Other areas in the building should be designed to be sterile.

Monitored Video Surveillance Systems (VSS) should be extended to cover the areas, where installed.

Refer to the Aviva Loss Prevention Standard **Management of Combustible Waste** for further guidance.

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.

- Flood protection Services - **Apex Flood Solutions**
- Flood risk management - **Ashfield Solutions**
- Flood risk assessments - **JBA Consulting**
- Fire risk assessment: **Cardinus Risk Management**
- Electrical/Lightning installation testing and explosion/DSEAR Risk Assessments: **Bureau Veritas**
- Thermographic imaging and PAT testing: **PASS**
- Automatic fire detection and portable extinguishers: **SECOM**
- Business continuity: **Horizonscan**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- LPS 1531: Issue 1.2 Requirements for the LPCB approval and listing of companies installing or applying passive fire protection products.
- EN 13501-1 Fire classification of Construction Products and Building Elements - Classification Using Data from Reaction to Fire Tests.
- BS EN 13501-2:2016 - Fire classification of construction products and building elements - Classification using data from fire resistance tests, excluding ventilation services
- LPS1208: LPCB Fire Resistance Requirements for Elements of Construction Used to Provide Compartmentation
- LPS 1500: Requirements for the LPCB Approval and Listing of Companies Installing Construction Elements Used to Provide Compartmentation in Buildings
- ASTM E2924-14(2020) Standard Practice for Intumescent Coatings
- CIRIA Code of Practice for Property Flood Resilience
- BS 85500: Flood Resistant and Resilient Construction – Guide to Improving the Flood Performance of Buildings.
- BS 851188: Flood Resistance Products - Building Products. Specification.

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:

- **Third Party Property Exposures**
- **Fire Compartmentation**
- **Fire Doors, Shutters, Dampers and Collars**
- **Data Centres - Cooling and Environmental Controls**
- **Data Centres - Escape of Water and Other Fluids**
- **Data Centres - Fire Detection and Protection**
- **Data Centres - 15 Top Tips**
- **Lithium-ion Batteries - General Considerations**
- **Electrical Installations - Inspection and Testing**
- **Lightning Protection**
- **Data Cabling**
- **Roof Mounted Photovoltaic Solar Panel Systems - General Considerations**
- **Roof Mounted Photovoltaic Solar Panel Systems - Planning for Installation**
- **Roof Mounted Photovoltaic Solar Panel Systems - Installation and Construction**
- **Roof Mounted Photovoltaic Solar Panel Systems - Installed and Ongoing Care**
- **15 Top Tips for Roof Mounted Photovoltaic Solar Panel Systems**
- **Grid-Scale Battery Energy Storage Systems - Construction**
- **Grid Scale Battery Energy Storage Systems - General Considerations**
- **Grid-Scale Battery Energy Storage Systems - Ongoing Care**
- **Small Scale Battery Energy Storage Systems**
- **Planning a Battery Energy Storage System - 12 Top Tips**
- **Electrical Lighting - Property**
- **Smoking and the Workplace**
- **Flood Guidance and Mitigation Global**
- **UK Flood Guidance and Mitigation**
- **Escape of Water and Other Fluids**
- **Escape of Water on Construction Sites**
- **Escape of Water - Installation and Maintenance**
- **Escape of Water - 10 Top Tips**
- **Work on Wet Systems**
- **12 Top Tips for Electric Vehicle Chargers and Electric and Hybrid Vehicle Charging**
- **Security - Computer Equipment**
- **Security - Doors and Windows**
- **Intruder Alarms - General Guidance**
- **Video Surveillance Systems - Introduction**
- **Cyber Security: Top 12 Tips to Protect Against a Cyber Attack**
- **Cyber Security: Ransomware**

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 1.1

ARMSGI3782026