Loss Prevention Standards – Asset Classes

Data Centres – Hazards and Ongoing Care

Version: 1.0

Date: 21st February 2025

This Loss Prevention Standard is one of a series of documents covering data centres, and specifically discusses the main hazards associated with data centres, and recommended controls to reduce the risks of loss or damage associated with these hazards.

AVIVA

Data Centres – Hazards and Ongoing Care

Introduction

Aviva Loss Prevention Standard **Data Centres – General Overview and Design Considerations**, the first in a series of documents covering data centres, provides an overview of the main activities, equipment, and design considerations, whilst **Data centres – Fire Detection and Protection** discusses the recommending methods of detecting and controlling fire via fixed protections.

This standard examines the main hazards associated with data centres and provides useful guidance on reducing the potential for loss or damage, and the associated business interruption losses, and ongoing care and maintenance.

Note: This document relates to data centres. It is not for on-site data processing and storage facilities, typically provided within business premises to support other trading activities, however, refer to 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

Businesses and organisations using data centre facilities are likely to have very significant reliance on them to support trading, accounting, servicing contracts and customer relations. It is critical the risks of damage and potential for loss are understood and managed by stakeholders.

Fire

The risks of fire can arise in a number of ways, but not limited to:

- **Overheating**. Server racks, Uninterrupted Power Supplies (UPS) equipment, and other associated equipment.
- **Cooling/Environmental**. Malfunctioning, overheating or failing cooling infrastructure.
- **Electrical**. Faults including lighting and surge, switchgear arcing and issues around demised responsibility for maintenance etc.
- **Lighting**. Some lighting systems can operate at very high temperatures and can result in catastrophic failure in the event of overheating or fault.
- **Heating**. Inappropriate heating may be used in offices, stores etc.
- **Hot Works**. Poor workmanship or mismanagement of hot tasks.
- **Battery Charging**. Fire can also originate within ancillary equipment, such as laptops and tablets, floor cleaning equipment and battery powered UPS equipment.
- **Arson**. Deliberate fire starting.
- **Emergency Power Generators**. Generator equipment will typically be located external to the data centre or within their own fire compartment within the same building. Combustion products such as smoke and burning brands can be drawn into air make up/ventilation and cooling systems, potentially damaging sensitive server and other IT equipment.
- **Transformer Fires**. Faulty or poorly managed equipment can result in ignition.
- **Exposures**. Hazardous activities or events in proximity can lead to contamination of the air supply and associated damage to sensitive equipment.
- **Smoking**. Smoking waste can come into contact with combustible materials, leading to ignition.

Fire can grow and develop, given the large, open nature of data halls, including floor and ceiling voids, combustibility of electrical cabling, insulation materials and the plastic components in use. It can also be exacerbated by the need for a strong clean fresh air supply to keep the data centre 'cool'.

Water and other Fluids

Fire is not the only concern, water related incidents, whether due to malfunctioning cooling equipment; localised flooding or pluvial exposures; leaks from damaged or compromised pipework or ingress from blocked or damaged guttering, routinely lead to loss or damage to key equipment and facilities being closed for repair. Data centres have traditionally utilised air cooling, which can develop condensate leaks, however in recent times liquid cooling systems have become more popular, as have evaporative cooling methods, both of which introduce liquids that can leak and lead to significant loss or damage.

Security

Data centres are highly secured environments however security breaches or damaged/faulty security protections can create vulnerabilities. Cyber security risks are increasingly prevalent.

Breakdown

IT related breakdowns and data loss can be costly and time consuming to resolve. Loss of revenues due to down time can be significant, if not catastrophic and attention to maintenance of systems, ancillary services such as cooling, and continuity planning are critical in this regard.

Business Continuity and Reputational Risk

The quality and speed of emergency response to loss related incidents can often be the factor which turns a small issue into a significant loss event and therefore failing to implement robust emergency procedures and business continuity arrangements can expose the organisation to potentially very large losses.

Finally, property damage losses can result in waste, contamination, and environmental impacts which negatively impact Environmental, Social and Governance (ESG) policies and reputations.

Hazard Management

Fire

Cooling issues. Guidance on cooling systems is provided in Aviva Loss Prevention Standard **Data Centres – General Overview and Design Considerations**.

- Cooling systems should be specifically designed for the data hall environments and the estimated heat output/electrical current draw.
  - ✓ Any changes to the layout of the data halls or wholesales changes/additional server equipment should result in the cooling provision being reviewed for adequacy and stepped up where necessary.
- Environmental monitoring systems, which provide essential cooling systems oversight, should include temperature monitoring; differential air pressure monitoring; humidity monitoring and leak monitoring.
  - ✓ Monitoring systems should be subject to formal maintenance, self-inspection checks and calibration as per Original Equipment Manufacturers (OEM) or installer guidelines.
- Ensure the cooling systems also reflect any future growth plans.
  - ✓ This helps avoid expensive downtime for infrastructure upgrades.
- Ensure emergency response planning to cooling system faults and issues has been documented and appropriate training provided to key workers.

Electrical hazards. The electrical system within the data centre should be designed, installed, and maintained in accordance with national regulations, codes, or standards.

- ✓ In the United Kingdom this is **BS 7671:2018+A3:2024 - Requirements for Electrical Installations. IET Wiring Regulations**.

- The work to be carried out by a competent contractor who is preferably a member of appropriate UKAS (United Kingdom Accreditation Service) installers and/or inspectors schemes.
- Ensure the electrical system reflects any future growth plans.
- Refer Aviva Loss Prevention Standard **Electrical Installations - Inspection and Testing** 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 reduced ignition hazards.
- Refer Aviva Loss Prevention Standard **Lighting** for further guidance.

Heating systems. Whilst the data halls are temperature controlled environments, ancillary areas such as offices, changing rooms and stores may feature localised heating.

- Ensure heating systems are appropriate and suitably managed for the location.
  - ✓ Adequate clearance should be maintained around heaters to prevent overheating of items in proximity.
  - ✓ Heaters should not be used to dry clothing.
    - Warning signage may be necessary if this has been noted in previous self-inspection audits.
  - ✓ Portable heating should not be used in any areas, this includes electrical fan and oil filled radiator types.
  - ✓ Ensure heating systems are subject to maintenance, servicing, and inspection in accordance with any national regulations, codes, or standards, and/or in accordance with manufacturers recommendations.

Hot Works. Formal contractor controls and arrangements for approving hot works, issuing, and signing off permits to work, ensuring works have been satisfactorily planned, carried out and completed, and all fire protections reinstated are in place.

Note: Hot works should always be the last resort within data hall areas and if required they should be closely managed in accordance with Aviva's **Hot Work Operations** Loss Prevention Standard.

Battery Charging. Lithium-ion battery powered equipment is likely to be present within data centres, most prominently within Uninterrupted Power Supply (UPS) battery systems, and guidance is provided later in this document. Other battery charging includes portable computers, floor cleaning plant, personal devices, electronic vaping devices, power tools for general maintenance etc.

The fire risks presented by such appliances should be risk assessed and appropriate control measures introduced.

- As a minimum, site rules should be issued in respect of the charging of personal devices e.g. only on non-combustible surfaces, during period of occupancy supervision and with adequate clearance from combustible items.
- Vape charging equipment should be prohibited from the premises.
- Charging cabinets with safety cutout protections are available for larger items such as power tool batteries and portable computers. Aviva Loss Prevention Standards – **Lithium-Ion Batteries - Portable Tools** and **Lithium-Ion Batteries – General Considerations.**

Aviva Specialist Partner Denios can assist with Charging cabinets.

Lightning Protection. Data centre buildings and the electronic equipment including monitoring and comms 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).
  - ✓ 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 effect protection needs of the building and vulnerable equipment.
- Any lightning protections 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 protections 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.

Exposure. An assessment of any risks presented by other buildings or occupancies in proximity to the data centre should be undertaken.

- 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 event.
- Contingency and emergency planning arrangements should be reviewed to ensure adequacy.
- Refer to Aviva Loss Prevention Standard **Third Party Property Exposures** for further guidance.

Electric vehicle Charging. Charging equipment should be located as far as possible from data centre buildings and other valuable assets, e.g. sprinkler tanks, generators, transformers. At least 10 metres is recommended.

- The battery systems on electric/hybrid vehicles can enter thermal runaway in the event of faults, damage or charging issues, typically resulting in volatile flaming/fire and explosion incidents.
- 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.
- Refer to Aviva Loss Prevention Standards **12 Top Tips for Electric Vehicle Chargers** and **Electric and Hybrid Vehicle Charging** for further guidance.

Smoking. Smoking should only be permitted within smoking shelters, located at least 10 metres from data centre buildings and other valuable assets. Ensure smoking waste is dampened before depositing in waste skips.

Housekeeping and Self Inspections

Good housekeeping standards are an essential component of effective risk management strategies. Contaminants such as pollen, air pollution, sea salt, dust, lint, skin particles, hair, food/drink, metal particles and fibres can lead to significant damage to sensitive equipment. As such, documented standards should be introduced specifying procedures and responsibilities with regards to housekeeping arrangements within the data centre.

These standards should detail matters such as:

- The type and frequency of cleaning regimes to prevent the build-up of any dust and other materials that could damage equipment, introduce additional fire hazards, increase the fire load or its continuity and potentially compromise the performance of any fixed firefighting systems.
  - ✓ A formal cleaning regime should be established detailing frequency and regularity of deep cleaning.
  - ✓ Monthly cleaning of server rack tops and other accessible ledges/surfaces.
  - ✓ Annual deep cleaning of plenums and floor voids.

- Prohibition of eating and drinking within data halls and other higher risk areas such as UPS rooms.
- The rules regarding the storage of combustible goods including spares, surplus equipment, filing, furniture etc.
- Access controls, e.g. authorisation procedures and the permitted activities.
- Rules should be in place in relation to compartment integrity e.g. ensuring any openings created during alterations/repairs, damage events etc., are repaired and fire stopped to the same fire resistance rating as the compartment, keys are removed from fire protection control panels etc.

A programme of inspections and audits should be carried out by trained individuals to monitor compliance and ensure that standards are maintained, and that data centre equipment is functioning correctly, and facilities remain in good repair with no signs of damage or faults, or water ingress. The frequency of inspections will vary between organisations, however in most cases weekly inspections are suitable.

- ✓ The use of photographic evidence with such inspections can prove invaluable.
- ✓ Thermographic camera inspections can also prove invaluable for such inspections. These are relatively inexpensive and can be used to check on the batteries in store or whilst the batteries are being test charged.

The Aviva Loss Prevention Standards **Housekeeping – Fire Prevention** and **Self-Inspections** provide useful guidance in this regard.

Backup Power

Systems Power Protection – Uninterrupted Power Supplies

Power outage is a critical risk exposure that requires careful management. Power loads 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.

Critical and essential loads are connected to an uninterruptible power supply (UPS) to provide protection from short term power outages. These are typically lithium-ion battery packs, which whilst acknowledged as safe can overheat, enter thermal runaway, and ignite when damaged, faulty, as a result of charging issues etc. To help minimise the effects of such an incident:

- UPS equipment should not be housed in the data halls. UPS equipment should only be installed within a separate room or compartment remote to the data hall environments.
- The fire resistance rating (insulation and integrity) of this room or compartment should reflect the expected fire growth and spread potential. In most cases at least 120 minutes is recommended.
- In addition to preventing the spread of fire, the safe management of smoke and gas emissions resulting from UPS lithium-ion battery fires, off gassing or thermal runaway should be assessed. Where a credible risk exists, mechanical ventilation systems to be installed, suitable for use in potentially explosive atmospheres.

  Note: This is of additional concern given the production of hydrogen gas that can be generated when firefighting water is applied to lithium-ion battery fires.

- The batteries within the UPS systems should provide sufficient backup time to allow standby generator equipment to start, and also to resolve any faults with automatic generator start up.
- The batteries in UPS systems should be monitored for charging, general performance/health etc., preferably via sensors to each battery within the system.
  - ✓ Response arrangements should be formalised for faults or alarms.
  - ✓ Use thermographic cameras to check regularly for hot spots/overheating within the battery system.

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

Standby Generators

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

- The generator(s) should be suitably sized to power all critical and essential loads within the data centre.
- Control systems should provide rapid synchronisation to ensure full power load is achieved promptly.
- Generators should preferably be located 10 metres from the data centre and not in proximity air intake systems.
  - ✓ Exhaust fumes may be drawn into the air inlets, potentially contaminating sensitive components.
- Separate fuel tanks should be at least 10 metres from the data centre.
  - ✓ Where there is a risk of leaking fuel damaging the data centre or drainage, bunding should be installed.
    - 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.
- Each data centre should have dedicated standby generator capability.
  - ✓ This ensures generators 'shared' by multiple data centres are not stretched beyond capacity in the event of significant power outage.
  - ✓ Consideration should be given to back up arrangements in the event of power failure. Duplicate generators, manual cross over to other generators at the site and/or install dual starting batteries, dual battery chargers and dual starter motors to each set to improve reliability.
- Generator equipment should be subject to regular formal maintenance by suitably trained persons in accordance with OEM or accepted best practice guidelines.

Note: The use of roof mounted Solar Photovoltaic PV systems and Battery Energy Storage Systems (BESS) are increasingly installed at business premises to generate and store electrical power. Other Aviva Loss Prevention Standards provide guidance in respect of such systems.

Water/Fluid Risk Controls

Data centres should not be located in an area vulnerable to flooding.

- Should the building be built above anticipated flood levels, foul water can still enter the building via drainage and sump systems during flood events, potentially damaging equipment and/or leading to electrical fires.
- The use of non-return/backwater valves should be considered on basement and ground level drainage systems.

Refer Aviva Loss Prevention Standards **Flood Guidance and Mitigation Global** and **UK Flood Guidance and Mitigation** for further guidance.

Aviva Specialist Partner Apex Flood Solutions can assist with flood mitigation planning and protection.

- Water services should not be present directly over data halls and should be diverted where present.
- Any condensate return pipework on air cooling systems should be located remote from or directly over the data hall areas.

- All water services within the building should be fitted with leak detection and flow monitoring equipment to detect pressure losses or unusual flow patterns, often indicative of escape of water events.
  - ✓ Leak detection points and water isolation stations should be detailed on a plan and shared with relevant personnel and displayed in a prominent location (typically alongside fire alarm and sprinkler plans).
  - ✓ Ensure appropriate emergency response training is provided to relevant workers to help ensure prompt isolation to water related events.

Aviva Specialist Partners Leaksafe and Quensus can assist with such protections.

- Water storage vessels, other than sprinkler tanks, should be stored external to the data centre, and where necessary bunded to ensure 110% of the contents would be captured in the event of failure or damage resulting in discharge.
- Do not locate bathrooms or other wet rooms directly over data halls, or where escaping water could track down into the facility.
  - ✓ Bathrooms are recommended at ground levels only and should be fitted with appropriate drainage so as to prevent water build up in the event of escape or leaks.
  - ✓ non-return/backwater valves should also be installed to drainage systems at ground and basement levels.
- External guttering should be designed so as to reduce the potential for blockages/overflowing into the building.
  - ✓ Guttering should also be accessible for ease of inspection and cleaning.

Maintenance

Date centre equipment, cooling/environmental systems, and the supporting infrastructure such as electrical installations; UPS systems; transformer and generator plant; passive fire features e.g. firestopping, fire shuttering etc.; fire detection and fire protection systems should be serviced and maintained in accordance with original equipment manufacturers (OEM), suppliers and installers recommendations. In respect of IT equipment this should include:

- **Hardware diagnostics**. Periodically checking hardware status and using automated system monitoring utilities to identify potential hardware errors.
- **Temperature**. Ensuring cooling systems are operating correctly and test heat alarms routinely.
- **UPS systems**. Ensure batteries are replaced prior to end of life/charging life expectations. Ensure any damaged UPS batteries are safely isolated and replaced as soon as possible.
- **Compartment integrity**. Ensuring firestopping and other passive fittings are maintained in good order.
- **Security audits**. Reviewing access and user accounts to avoid security breaches and identifying any potential security risks. Change any security codes to digital door locks, safes, intruder alarm controls.

Security

A security assessment should be undertaken, and appropriate protections considered including:

- Good quality perimeter protections 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.
- Video Surveillance Systems (VSS).
- Intruder and holdup alarm provision.
- Cyber security arrangements.

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**

Business Continuity

Every business should have a formal Business Continuity Plan in place. This should be reviewed to ensure disaster recovery and continuity arrangements remain adequate. Any actions generated should be addressed promptly.

Emergency Response

Given the risks associated with data centres, an emergency response plan should be produced specifically developed to outline key responsibilities and actions in an emergency event. The emergency response plan should include best practice responses to all likely property and business interruption risks including fire; electrical damage including lightning and surge related events; UPS or BBU lithium-ion battery fires/thermal runaway; escape of water and other fluid related exposures; security/theft damage.

The emergency response rules should be formally documented, and appropriate training provided.

Key Action Steps

- Ensure the data centre has an appropriate fire resistance rating (insulation and integrity).
- Fire protection and detection systems should be bespoke to reflect the sensitivity of the equipment and processes. Ensure your Property Insurer and Broker are engaged as soon as possible.
- Monitoring should be in place in respect of cooling and environmental systems with response procedures formalised.
- Manage escape of water/fluid risks:
  - ✓ Ensure water services are not installed directly over, or in proximity to data halls where there is foreseeability of water leaks breaching data halls and other key areas.
  - ✓ Install bathrooms at ground level and tank/drain to ensure water cannot pool/accumulate and spread to high risk areas.
  - ✓ Water storage vessels should be installed externally and bunded if necessary.
- Ensure formal cleaning arrangements are in place and adopt strict housekeeping standards.
  - ✓ Data centres should be maintained as sterile areas wherever possible. Dust can also impact some fire protection systems.
- Complete at least weekly self-inspections to ensure housekeeping expectations are maintained and facilities, including cooling systems and fire detection and protection systems, are operating normally with no signs of damage, faults, or water ingress/escape of water.
  - ✓ Use thermographic cameras to check for water ingress and overheating components.
- Adopt emergency procedures and provide appropriate training to workers and contractors.
- Review Disaster Recovery and Business Continuity plans, ensuring back up arrangements are in place.

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, including:

- **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**
- **Leak detection: Leaksafe**
- **Leak detection and Flow monitoring: Quensus**

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

Sources and Useful Links

- The Dangerous Substances and Explosive Atmospheres Regulations 2002.
- BS EN 62305 - Protection against lightning.
- BS 7430:2011+A1:2015 Code of Practice for protective Earthing of Electrical Installations.
- BS 5839-1:2017 - Fire detection and fire alarm systems for buildings - Code of practice for design, installation, commissioning, and maintenance of systems in non-domestic premises.
- LPS 1204 : Issue 3.2 Requirements for Firms Engaged in the Design, Installation, Commissioning and Servicing of Gas Extinguishing and Condensed Aerosol Systems.
- British Standard BS5306 – Fire Extinguishing Installations and Equipment on Premises.
- BS EN 16750:2017+A1:2020Fixed firefighting systems. Oxygen reduction systems. Design, installation, planning and maintenance.
- Loss Prevention Standard LPS 1197: Issue 4.2 Requirements for the LPCB approval and listing of companies inspecting, repairing, and maintaining fire and security doors, door sets, shutters, and active smoke/fire barriers.
- BS EN 15004 - Fixed firefighting systems. Gas extinguishing systems.
- BAFE Scheme SP101 Competency of Portable Fire Extinguisher Organisations and Technicians.
- British Standard BS5306 – Fire Extinguishing Installations and Equipment on Premises.
- BS 8489-1:2016 Fixed fire protection systems – Industrial and commercial watermist systems Part 1: Code of practice for design and installation.
- BS EN 14972-1:2020 Fixed firefighting systems – Water mist systems Part 1: Design, installation, inspection, and maintenance.
- LPS 1230 – 1.2 Requirements for fire testing of fixed gaseous fire extinguishing systems.
- BS ISO 14520-1 Gaseous fire-extinguishing systems – Physical properties and system design – Part 1: General requirements.
- BS EN 16750:2017+A1:2020 Fixed firefighting systems. Oxygen reduction systems. Design, installation, planning and maintenance.
- LPS 1531: Issue 1.2 Requirements for the LPCB approval and listing of companies installing or applying passive fire protection products.
- BS7273:2006 Electrical actuation of gaseous total flooding extinguishing systems.

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:

- **Gaseous Fire Extinguishing Systems**
- **Water Mist Fire Protection Systems**
- **Property and Business Impact Risk Assessment**
- **Self-Inspections**
- **Fire Compartmentation**
- **Escape of Water and Fluid Leakage**
- **Fire Safety Legislation**
- **Electrical Installations - Inspection and Testing**
- **Housekeeping - Fire Prevention**
- **Maintenance Regimes**
- **Heat and Smoke Venting Systems**
- **Hot Work Operations**
- **Managing Change - Property**
- **Thermographic Surveys**
- **Managing Contractors**
- **Business Continuity**
- **Power Outage**
- **Roof Mounted Photovoltaic Solar Panel Systems - General Considerations**
- **Roof Mounted Photovoltaic Solar Panel Systems - Planning for Installation**
- **Roof Mounted Photovoltaic Solar Panel Systems - Isolated End of Life and Decommissioning**
- **Roof Mounted Photovoltaic Solar Panel Systems - Installed and Ongoing Care**
- **Roof Mounted Photovoltaic Solar Panel Systems - 15 Top Tips**
- **Roof Mounted Photovoltaic Solar Panel Systems - Installation and Construction**
- **Small Scale Battery Energy Storage Systems**
- **Grid Scale Battery Energy Storage Systems**
- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks**
- **Cyber Security: Respond and Recover**
- **Cyber Security: The Internet of Things**
- **Ransomware – Cyber Loss Prevention Standard**

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.

21st February 2025

Version 1.0

URN - ARMSGI2272024

LOSS PREVENTION STANDARDS