Loss Prevention Standards – Asset Classes

Server/Comms Rooms

Version: 1.0

Date: 30th September 2024

The safe and effective management of data is critical to many organisations. Online commerce, invoicing, distribution modelling etc., all rely on critical IT infrastructure.

This Loss Prevention Standard provides guidance on reducing the risks of loss or physical damage to server/comms rooms and equipment, and the associated impacts to trading.

Server/Comms Rooms

Introduction

Server/comms rooms 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.

With many businesses and organisations utilising such facilities within their premises, and with significant reliance on these to support main business activities e.g., sales, invoicing, accounting, contracts and agreements, customer service, administration systems etc., it is critical the risks of damage and potential for loss are understood and managed by relevant stakeholders.

Server/comms rooms can be vulnerable to damage, with causes of loss including fire, smoke, escape or ingress of water/other fluids, security breaches and the business continuity losses associated with physical damage to such equipment/facilities. For example a server room fire at a council chambers property in Edinburgh in November 2023 led to extensive damage and closure of the building, which also hosts weddings and civil ceremonies, and was closed for several days to allow for repairs. The risk management guidance within this Loss Prevention standard can help reduce the risks of such incidents.

Note: This document relates to server/comms rooms, typically provided within business premises to support other trading activities. It is not to be used for those occupancies who are primarily classed as data centres. The focus is towards property loss prevention and related risk management guidance and is not intended to address liability exposures. The presumption is that all regulatory requirements, such as Fire Risk Assessments, have been met.

Understanding the Risks

Server/comms rooms typically feature:

- Network Systems - The network system connects:
  - ✓ On-site server equipment that both processes and stores data, to other owned and third-party facilities and to other end user locations.
- Storage Systems – Used to store/maintain the data.
- Computing Systems – The servers which process, locally store, administer and manage the data.
- Ancillary systems – Heating/cooling systems, electrical installations, telecommunications, security hardware, fire detection and fire protection systems etc.

The potential causes of loss or damage are varied and include, but are not limited to:

Fire and Smoke Damage

The risks of ignition are continually present and can arise from:

- Overheating components or ancillary equipment.
- Overloaded power outlets.
- Defective IT equipment.
- Malfunctioning or overworked cooling and heating equipment.
- Battery faults in UPS systems or other battery powered equipment under charge.
- Damaged or defective lighting.
- Lightning and surge events.
- Poor workmanship or mismanagement of workplace tasks e.g. hot work.

Fire spread can be aided by:

- Poor housekeeping such as stored goods and spares, filing, furniture etc.
- Inadequate fire stopping which may allow the fire to spread beyond the server/comms room, and potentially through the property, or from the wider property into the room.
- Inadequate or faulty fire protections and automatic fire detection systems, which can lead to potential delays in responding to fires, leading to more extensive damage.

Water and Other Fluids

Fire and smoke are not the only concern, water and other fluid related incidents can arise due to:

- Damaged or defective cooling equipment.
- Leaks from damaged or compromised pipe work from within, adjacent to, or above server/comms rooms.
- Ingress from blocked or damaged guttering.
- Heavy rainfall, localised flooding, and overflowing drainage, particularly in respect of basement or ground floor located facilities.
- Spilt drinks.

Security Risks

The IT/comms equipment may be attractive to thieves and the security measures implemented may be critical in protecting against physical loss, data security breaches and reputational damage. Issues include:

- Poor, or inadequate physical security, e.g. door and window locks, security cages and cables, and security grilles and shuttering etc.
- Inadequate access control arrangements.
- Compromised intruder alarm protection.
- Shielded or damaged video surveillance systems.

Business Continuity and Reputational Risks

The quality and speed of emergency response to loss related incidents can often be the factor that helps prevent a small issue becoming a significant loss event. Failing to implement robust emergency procedures and business continuity arrangements can expose the organisation to potentially larger than expected losses. Property damage losses can also result in waste, contamination, and environmental impacts which negatively impact Environmental, Social and Governance (ESG) policies and reputations.

Risk Assessment / Impact Analysis

Risk Assessment

Ensure all relevant regulatory and business focussed risk assessments, including the premises Fire Risk Assessment have been reviewed to assess the fire exposures related to server/comms rooms and ensure fire safety and fire protection arrangements remain adequate. Any actions generated by risk assessment should be addressed promptly.

Any emergency fire information left at the premises for the emergency services should also be updated to confirm:

- The possible presence and location of lithium-ion batteries in Uninterrupted Power Supply (UPS) and/or Battery Backup (BBU) systems,
- Any areas with automatic fire protection systems, particularly those that might affect oxygen levels.

Business Impact Analysis

A Business Impact Analysis (BIA) should be conducted to help understand the exposures created by server/comms rooms and help with risk control planning. The BIA should include:

- Input from all departments or business teams and a review of the systems, equipment and applications required to carry out their role functions.
- A criticality assessment of these role functions and various business drivers including revenue/profitability, productivity, legal/contractual, safety, reputational and ESG perspectives.
- An assessment of how often data is input into systems and the impacts a loss of data processing and storage facilities would have to core/critical functions across a range of potential 'downtime' periods e.g., 60 minutes, 3 to 6 hours, 12 to 24 hours, 24 hours plus etc.
- An assessment of maximum tolerable downtime (MTD) for each core/critical business function.
- Approval of the BIA findings by the senior management team. Department heads or team leaders may over emphasise the criticality of some processes within their operational areas or downplay the criticality of functions within other departments or teams.
- An assessment of the likely source of loss or damage that might affect server/comms rooms. These may be sources within the facility, wider premises or third-party locations in proximity, particularly hazardous activities such as bulk liquid or flammable materials/agent storage/handling, hazardous cooking etc.
- An assessment of the fire load within the facility e.g., combustible surfaces or linings, storage of combustible goods, extensive use of non-fire rated plastic components such a PVC cabling etc.
- Vulnerable periods such as during peak season trading, periods of unoccupancy where no immediate emergency response can be provided.

The BIA should help identify the critical functions, equipment and applications needed to maintain ongoing operations; the likely scale of damage or loss arising from any risk event; and provide the basis for designing and protecting server/comms rooms to reduce, manage, and mitigate loss potential.

Business Continuity Planning

In tandem with the BIA, the existing Business Continuity Plan should be reviewed to ensure disaster recovery and continuity arrangements remain adequate. Any actions generated should be addressed promptly. Please refer to the Aviva Loss Prevention Standard **Business Continuity** for further guidance.

Management of Change

Any proposed changes to business activities should also be managed through a formal Management of Change process, to help ensure all stages of the change are progressed with the minimal exposure to the existing arrangements e.g., changes to layout to accommodate the facility/facilities, new air conditioning equipment or re-cabling, and any necessary risk management controls. These proposed changes should also be discussed with your Property Insurer and Insurance Broker. Please refer to the Aviva Loss Prevention Standard **Managing Change** for further guidance.

Management Policy and Standard Operating Procedures

A management policy should be introduced in relation to all server/comms rooms. This policy should be clearly communicated to all employees, and other applicable stakeholders e.g., visitors, contractors etc.

Standard Operating Procedures (SOPs) and Emergency Operating Procedures (EOPs) detailing key responsibilities; security access; key operations; maintenance and inspections; training and emergency arrangements etc., should be produced, shared with relevant employees, and reviewed regularly. The formalisation of clear rules and procedures helps to ensure consistent and safe processes and procedures are followed by relevant personnel, reducing the risks of unplanned and unexpected fires or other property damage events, and mitigating the losses associated with poor or unclear emergency planning.

Employee's and other relevant persons should be actively encouraged to report any incidents or issues involving property damage including physical damage to the facility and equipment; fire protection equipment and room integrity issues such as damaged door seals; unsafe or unauthorised activities; security arrangements/security breaches; signs of water ingress however minor; inappropriate storage etc., to a responsible person within the business for review.

Room Location and Design

- Choose upper floor locations for siting of server/comms rooms where possible. This reduces the potential for 'rising water' related damage attributed to localised flooding, heavy surface water ingress, drainage issues etc., and water filled services leaking on upper levels down into basements and ground floor locations.
- Do not position facilities in proximity to hazardous trade activities or environments such as hazardous cooking environments e.g. canteen facilities with deep fat frying equipment, flammables goods storage/handling rooms, welding/fabrication workshops etc. An incident in such an environment may develop quickly and potentially spread to the adjacent facility.

Fire Resistance

All server/comms rooms should be:

- Of non-combustible construction providing a fire resistance rating, including the ceiling/ceiling tiles, raised flooring and glazed elements of at least 60 minutes (insulation and integrity).
    - ✓ Fitted with appropriately tested and accredited automatically closing fire door(s), providing fire resistance (insulation and integrity) rating consistent with the construction. These fire doors to be kept closed at all times.
    - ✓ **Note:** The provision of any doors for the room, should not compromise the ventilation systems or any fire suppression systems within.
- Any penetrations and/or openings for cabling and pipework etc., should be adequately firestopped and/or fitted with intumescent collars with materials providing a fire resistance rating consistent with the construction.
    - ✓ Intumescent collars should be used to protect pipework which could collapse or melt in the event of fire, filling any voids created and providing a fire barrier.
    - ✓ The use of intumescent pillows for temporary fire stopping around service openings is not recommended unless limited to very short time periods e.g., temporary passive fire protection during a planned change to the facility.
- Installation of other passive fire protection products such as firestopping should be completed in the United Kingdom by a company certificated to a third-party competency scheme, such as LPCB Loss Prevention Standard - LPS 1531: Issue 1.2 Requirements for the LPCB approval and listing of companies installing or applying passive fire protection products. In other territories, a local equivalent International Standard should apply.
- UPS or BBU equipment should not be housed in the same compartment as server/comms equipment. This equipment to be installed within a separate room or compartment remote to the facility.
    - ✓ 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 60 minutes is recommended, however higher fire resistance ratings should be considered where the exposures to the facility are too high or to address actions stipulated in the premises Fire Risk Assessment.
    - ✓ In addition to preventing the spread of fire, the safe management of smoke and gas emissions resulting from UPS/BBU 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.

Fire Protections

Automatic Fire Detection

- Automatic fire detection should be provided and be compliant with relevant standards. In the United Kingdom, category L1 or P1 of BS 5839-1 - Fire detection and fire alarm systems for buildings - Code of Practice for Design, Installation, Commissioning, and Maintenance of Systems in Non-Domestic Premises. In other territories, a local equivalent International Standard should apply.
- Given the critical dependencies on server/comms rooms, the use of high sensitivity aspirating detection technology, which can provide very early warning of fire events is recommended.
- The detection should extend to any floor or ceiling voids, and guidance should be obtained from an accredited fire alarm installer where required.
- The number, type, and location of the detectors within the room and any voids should be based on the expected air velocities and air movement characteristics. In many server/comms rooms the ventilation systems can provide high velocities, stratified air layers or stagnant air pockets (in the room corners) etc. As a result, in many cases the use of a cold smoke pencil should help establish the air movements within the room.
- A means of manually raising the fire alarm should also be provided, inside and outside of the room.

Any plans to change the existing fire detection system or install a new fire detection system should be discussed with your Property Insurer and Insurance Broker.

Automatic Fire Protection

Based on the Business Impact Assessment and the exposed values, automatic fire protection should be considered for server/comms rooms and adjacent UPS/BBS areas.

If any automatic fire protection system is planned for any server/comms room, please contact your Property Insurer and Insurance Broker to discuss specification and design requirements.

There are a number of fire protection systems that may be suitable for server/comms rooms including:

Automatic Sprinklers

- Sprinkler systems are the most reliable means of suppressing fire at its seat and limiting the extent of fire damage and impacts to trading. Where installed at the premises, the sprinkler system should be extended to protect the server/comms room.
- Consideration should be given to the most appropriate system design for the room.
    - ✓ A wet pipe sprinkler system is the most reliable sprinkler system and has the least amount of delay before water can suppress a fire at its seat.
        - With this system design the sprinkler pipework is normally charged with water, and as soon as the fire activates a sprinkler head in the room, water is immediately available to suppress the fire at its seat.
        - Utilising concealed or institutional sprinkler heads in the server/comms room would significantly reduce the potential for impact related damage to sprinkler heads. This is a cause of sprinkler leakage in such areas.

- ✓ A single interlock pre-action system might be suitable, depending on the criticality of the server/comms room and any expected delays in replacing and reinstating equipment and data.
    - With this system design the sprinkler pipework is normally charged with a low pressure supervisory air supply.
    - The sprinkler pipework only charges with water when the automatic fire detection within the server/comms room goes into alarm.
    - Ideally, this should be when a single automatic fire detector goes into alarm (single knock) but can be upon alarm of two fire detectors (double knock).
    - Water is only discharged from the system when the fire activates a sprinkler head in the room.
- ✓ A double interlock pre-action system is not normally recommended. Unlike a single interlock system, water is only charged into the sprinkler pipe when both the automatic fire detectors in the room alarm and a sprinkler head in the room fuses.
- ✓ A dry pipe sprinkler system.
    - With this system design the sprinkler pipework is normally charged with an air supply (higher than a pre-action system), and as soon as the fire activates a sprinkler head in the server/comms room, the air is ejected from the open head and water is charged into the system.

Inerting Gaseous Fire Extinguishing Systems – Automatic

- A blend of gases, typically argon, Co2 and nitrogen, are released upon detection of a fire, which deplete oxygen levels in the room and knock down the fire. Refer to Aviva Loss Prevention Standard **Gaseous Fire Extinguishing Systems** for further guidance.

Clean Agent Suppression Systems

- The systems utilise chemical agents under pressure to suppress fire, without significantly reducing oxygen levels in the room.

Watermist Fire Protection Systems

- Occasionally used in server/comms rooms, these systems emit finely divided water droplets under pressure through small orifice nozzles to produce a mist. This mist thermodynamically cools the fire via evaporation of the water particles and reduces the oxygen within the compartment by steam displacement.

Hypoxic Air

- Also known as oxygen reduction systems, these operate by maintaining oxygen levels within the facility below 15% by volume via the separation of oxygen from the atmosphere thereby increasing the volume of nitrogen gas and reducing the probability of ignition.

Note: Any room protected by a gaseous suppression system must be capable of holding the inerting agent to suppress the fire for a specified time period, and a Room Integrity Test must be undertaken at the commissioning stage, after any changes to the room and annually as part of ongoing routine maintenance, to ensure compliance.

Note: Any server/comms room protected by a gaseous suppression system must consider the impact of the ventilation arrangements serving the room. Is this:

- Interlocked to shut down before the extinguishing agent discharges?
- 100% fresh air inlet and full exhaust?
- Recirculating with a percentage of exhaust and fresh air make-up?
- 100% recirculating only?

This will impact the system design and performance.

Note: One consistent failing of local fire suppression systems in server/comms rooms is 'panel' key management. Fire suppression system panel keys should not be left in situ in the panel. Panel keys should be kept in a secure area and there should be a formal key management process for authorised individuals who need to access the panel key. The management of suppression systems from automatic to manual status requires strict control.

Note: Whilst localised, automatic, fire protection systems, that protect the server/comms room only are beneficial, from a fire starting in that room, they do not protect the whole property. A fire originating in another part of the building, not benefitting from any fire suppression or automatic sprinkler coverage may well develop and lead to a significant, or catastrophe loss event. As a result, automatic sprinkler protection provides whole property protection and is recommended in most cases.

Alarms

Alarms associated from the above should raise a site fire alarm to ensure there is an appropriate emergency response and escalation if needed. If not already in place, the alarm system on site should be connected to a constantly attended location or an approved Alarm Receiving Centre. An accredited fire alarm installer can provide further guidance and assistance.

Note: Any the alarms associated with any fire suppression systems, including fault; out of automatic and fire, should also be connected to a constantly attended area.

Interlocks

The use of interlocks is critical in server/comms rooms to help reduce the potential for fire and smoke damage. As such, the actuation of any of fire detection/alarm and protections systems should be interlocked to:

- ✓ De-energise the power supplies.
- ✓ Isolate charging equipment.
- ✓ Automatically close any fire doors.

In many cases interlocks to the ventilation and any smoke management systems may also be provided. This is particularly important where the server/comms room is protected by a gaseous extinguishing system.

Any interlocks should be tested at least annually and restored following any impairment to the fire detection/alarm and protection systems.

Enabling Devices

An enabling device may be installed to 'hold off' the discharge of a fire suppression system within server/comms rooms. If this is provided, this must be located within the protected area itself and not outside of the room.

Manual Fire Extinguishers

- Ensure appropriate numbers of fire extinguishers are present within the facility suited for use on electrical fires and other classes of fire within the facility.
- Whilst dry powder type appliances may be suitable for such facilities, damage caused by residues to non-affected equipment can be extensive and are therefore not recommended.

The Aviva Loss Prevention Standard **Fire Extinguishers - Selection, Location and Servicing** provides guidance on the number, type, location of appliances along with guidance on selecting a competent installer.

Housekeeping

Good housekeeping standards are an essential component of effective risk management strategies.

As such the server/comms room should only contain the designated equipment and essential non-combustible items of furniture.

Note: Server/comms rooms should not be utilised for storage including spares, stocks, surplus furniture, laptop stores, filing etc. These should be stored in other dedicated storage rooms.

You should also ensure:

- Eating and drinking is prohibited within the server/comms room.
- Access controls are limited to authorised personnel only.
- Formal contractor controls and arrangements for approving works, issuing, and signing off permits to work, ensuring works have been satisfactorily completed, and all fire protections reinstated are in place.

  Note: Hot works should always be the last resort within server/comms rooms and if required they must be closely managed in accordance with Aviva's **Hot Work Operations** Loss Prevention Standard.

- Rules on room integrity, ensuring any openings created during alterations/repairs, damage events etc., are repaired and firestopped to the same fire resistance rating as the compartment, keys are removed from fire protection control panels etc., are in place.
- Fire detection devices and fire protection equipment should be inspected weekly to ensure they are not covered, blocked, impaired, painted, damaged etc.
- A formal cleaning regime is in place to prevent the build-up of any dust and waste materials that could introduce additional fire hazards, increase the fire load or its continuity and potentially compromise the performance of any fixed firefighting systems.

Self-Inspections

- A programme of inspections should be carried out by trained individuals to monitor compliance and ensure that standards are maintained, and that server/comms rooms are 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 electrical equipment, lighting, ventilation and cooling and any UPS or BBU systems in adjacent compartments. Refer to Aviva Loss Prevention Standard **Thermographic Surveys** for further guidance.

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

Lightning Protection

- Buildings, server/comms rooms, and the electronic equipment 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), and any lightning protection systems should be installed in accordance 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 all server/comms rooms.
- 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.

Water Exposure and Other Fluids

- Choose upper floor locations for siting of server/comms rooms where possible. This reduces the potential for 'rising water' related damage attributed to localised flooding, heavy surface water ingress, drainage issues etc., in basements and ground floor locations.
- Check building plans for water services within the room and divert where possible.
- Floor voids in server/comms rooms should not be used to house water/liquid carrying services.
- Do not locate server/comms rooms directly under any bathrooms or water storage vessels where escaping water could track down into the facility.
- Tanking the floors of any rooms holding water services directly above or adjacent to server/comms rooms can help prevent water ingress.
- Leak detection should be installed to any water services present.
- Regularly check for evidence of water staining to ceilings, which may suggest ongoing water ingress and potential for further water related incidents.
- Check external guttering locations and the potential for blockages and overflowing into the facility.

General Infrastructure and Ancillary Considerations

Redundancy

- All server/comms rooms should be designed to provide sufficient back-up systems and components that can take over immediately should the primary system fail. This can help reduce the impact of outages, ensuring that services remain available, and downtime is minimised.
  - ✓ If the business impact is too great this should also include diverse routing or protected routing for power and data cables.
- It is important to include other associated systems such as heating, cooling, air handling, fire protections etc., when considering redundancy arrangements.

Cooling

- The server/comms rooms will require appropriate cooling systems to maintain system performance and reduce the potential for overheating.
- For small facilities standalone, portable or wall mounted air conditioning units may be appropriate. These are simple to install and have the advantage of providing cooling where most needed.
- Fixed systems should be designed and the cooling requirements, calculated by a competent company.
- Perimeter or 'In Room' cooling designs use Computer Room Air Conditioners (CRAC) positioned around the perimeter of the room and utilise raised floor voids to deliver cold air around the facility. The cold air is pushed around the room by the CRAC units under the floor and released or delivered through ceiling ventilation.
- The cooling systems designer and the installers of any fire detection and fire protections should consult to ensure the air movements do not impact performance of the fire systems.
    - ✓ Aviva have noted incidents where rapid air speeds and/or air stratification would delay activation of the fire detection and protection systems.
- Room temperatures should be monitored and building management systems should provide adequate alarms in the event of high temperature thresholds being achieved/exceeded.
    - Suitable emergency response arrangements should be in place to respond to high temperature events (including outside of operating hours) such as supplementary portable cooling equipment, isolation of non-critical equipment etc.
- The condensate and return cycles should be considered for an escape of water risk assessment and exposure management.

Cabling

- To help reduce the potential for cable related fire damage, fire resistant cabling should be used wherever possible, or fire resistant cabling where a fire resistant option is not available. Please refer to the Aviva Loss Prevention Standard **Data Cabling** for further guidance.
- Implementing a cable management plan for ethernet, fibre-optic, power, and patch cables can prevent electrical shorts and fires. This includes organizing cables neatly, conducting regular inspections, and timely replacement of frayed or damaged cables.
- Power and data cabling should be run in separate cable trays/trunking.
- Minimising cables on floors can help prevent the risks of general wear and tear and water related damage in the event of escape of water incidents.
- All redundant and legacy cabling should be removed, and any openings fire-stopped to the same fire resistance rating as the server/comms rooms.

Efficiency

- Overworking or overloading the data processing, storage and ancillary systems can contribute to breakdowns, longevity issues and performance concerns.
- Where possible increasing the capacity via additional data equipment, servers, cooling systems etc., and reducing the operating requirements of each component in the system can reduce the potential for breakdowns as well as reducing replacement, repair, and cooling costs.

Maintenance

Data processing equipment, data networks, storage systems and the supporting infrastructure such as electrical installations, UPS and/or BBU systems, air conditioning, fire detection and fire protection systems should be serviced and maintained in accordance with original equipment manufacturers (OEM), suppliers and installers recommendations or appropriate national standards. Maintenance in respect of hardware should include:

- **Temperature/Cooling**. Ensuring cooling systems are operating correctly and heat alarms tested routinely. Check routinely for water/fluid leaks.
- **Dust.** Clean and remove dust from around equipment and ports.
- **UPS and BBU systems**. Ensure batteries are replaced prior to end of life/charging life expectations. Ensure any damaged UPS and BBU batteries are safely isolated and replaced as soon as possible.
- **Hardware diagnostics**. Periodically checking hardware status and using automated system monitoring utilities to identify potential hardware errors.
- **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.
- **Data backups.** Ensuring that data is backed up regularly to protect against data loss in the event of a disaster recovery scenario.

Security Arrangements

A security assessment of all server/comms rooms should be undertaken, and appropriate protections considered including:

- Use of upper floor locations where possible. Siting facilities on upper floors adds 'layers' of protection via access control to floors, rooms etc., and can help deter or hinder attempted security breaches.
- Good quality perimeter protections e.g., site fencing and secured vehicle and pedestrian gates.
- Authorised access control to the building and all server/comms rooms including systems to remove authorisation immediately upon persons leaving the business, or who are no longer authorised to access the facility.
- Property, facilities and/or security management should also have security access, should an emergency occur when IT teams are not present on site.
- Good quality key operated locks to windows. In some cases, additional physical security barriers may be required to some windows, particularly those providing direct access to facilities. Internal/external steel bars; fixed or removable steel mesh grilles; roller shutters or internal collapsible (folding) grilles may be considered.
- 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 – Guidance for Customers**
- **Security - An Introduction to Closed Circuit Television (CCTV) Systems**
- **Cyber Security: Top 12 Tips to Protect Against a Cyber Attack**
- **Cyber Security: Ransomware**

Emergency Response

Given the risks associated with server/comms rooms, 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.

Impairments

Ensure any impairments relating to fire detection, fire protection and security systems are reported to your Property Insurer and Insurance Broker. Temporary changes may be necessary to some arrangements whilst impairments are ongoing.

Key Action Steps

- Ensure relevant Risk Assessments have been reviewed to include the presence of all server/comms rooms.
- Conduct a Business Impact Analysis (BIA) to help identify the critical functions, equipment and applications, the likely scale of damage or loss and the necessary risk controls and protections.
- Produce and share a Management Policy with clear rules within Standard Operating Procedures.
- Ensure all server/comms rooms achieve a specific fire resistance rating (Insulation and integrity), e.g., 60 minutes or more as required or specified in the premises Fire Risk Assessment, and routinely inspect facilities for breaches and fire stop as necessary.
- Re-route water services within and in proximity to server/comms rooms. Bathrooms or room housing water storage vessels should be tanked if there is potential for leaks and ingress into the facility. Routinely check guttering where blockages and overflowing could lead to water ingress.
- Maintain server/comms rooms as sterile areas with no internal storage.
- 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.
- Seek advice from your Property Insurer and Insurance Broker when considering automatic fire detection and fire protection systems. Ensure automatic detection and fire protection extends to floor and ceiling voids and ensure keys are removed from control panels.
- Introduce emergency procedures and provide appropriate training to staff and contractors.
- Review Disaster Recovery and Business Continuity plans, ensuring back up arrangements are in place.

Checklist

A generic **Server/Comms Room Checklist** is available which can be tailored to your own organisation.

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**

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

Sources and Useful Links

- The Dangerous Substances and Explosive Atmospheres Regulations 2002.
- The Regulatory Reform (Fire Safety) Order 2005.
- The Fire Safety (Scotland) Regulations 2006.
- The Fire (Scotland) Act 2005.
- The Fire and Rescue Services (Northern Ireland) Order 2006.
- 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.**
- **Business Impact Analysis.**
- **Property and Business Impact Risk Assessment.**
- **Fire Safety 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.**
- **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.

30th September 2024

Version 1.0

URN - ARMSGI2072024

LOSS PREVENTION STANDARDS