Server/Comms Rooms - Checklist

Version: 1.0
Date: 30th September 2024

Server/Comms Rooms - Checklist

Location	
Date	
Completed by (name and signature)	

	General Overview	Y/N	Comments
1.	• Have significant planned changes to the premises layout to provide data processing and storage facilities been discussed with your Insurer and Broker? • If so, has any related guidance or risk improvements been actioned or scheduled for action?		
2.	• Is there a Management Policy and Standard Operating Procedures in place detailing operating requirements/rules, key responsibilities, emergency arrangements etc? • Have these been shared with relevant staff? • Are arrangements in place for regular reviews?		
3.	• Does the business/site have a formal Management of Change process? • Where relevant, have the planned changes to the premises layout to provide data processing and storage facilities been reviewed through this process?		
4.	• Have all appropriate existing risk assessments, such as a Fire Risk Assessment and an explosive atmospheres/DSEAR assessment been revised and updated? • **Have the life safety risks associated with any oxygen reducing fire protections been considered within the premises Fire Risk Assessment?** • If so, have recommended remedial actions been implemented or scheduled for implementation?		

LOSS PREVENTION STANDARDS

			Y/N	Comments
5.	•	Have you updated any emergency fire information located at the premises for the emergency services to confirm the presence and location of any lithium-ion batteries with UPS and/or BBU systems?		
	•	Are emergency response procedures in place relating to: ▪ Fire events? ▪ Escape of water or other fluid related incidents? ▪ Failure or fault with cooling systems? ▪ Security breaches? ▪ UPS/BBU battery incidents e.g., damage, fault, off gassing etc? • is there an escalation process to ensure prompt remediation by appropriate members of staff and management?		
6	• • • •	Has a Business Impact Analysis (BIA) been completed? If yes, has this been reviewed in recent years? Have all departments and business teams been included in the BIA? Have any actions generated in the BIA been implemented or scheduled for implementation?		

Design			Y/N	Comments
7.	• • • •	Are all rooms or halls housing data processing and storage facilities achieving a fire resistance rating of at least 60 minutes (insulation and integrity), or more where specified by Insurers or within the premise Fire Risk Assessment? Are floating floors and ceilings of non-combustible construction? Are all entrance doors rated to provide to provide the same fire resistance rating? Are there arrangements in place for reviewing fire stopping is installed post any works creating openings or otherwise compromising the fire resistance rating of the room?		
8.	• •	Has an explosion/ DSEAR Assessment been completed or recently reviewed in respect if lithium-ion battery UPS and/or BBU systems? If yes, have any recommended remedial actions been completed or scheduled?		

LOSS PREVENTION STANDARDS

9.	• Are any UPS or BBU systems located in separate fire rated compartments to the data processing and storage facilities? • Is this compartment adequately cooled? • Are there arrangements to replace batteries before end of life/charging life cycle thresholds are achieved?		
10.	• Are any mechanical ventilation systems within UPS and/or BBU rooms rated as suitable for use in potentially explosive atmospheres?		
11.	• Are data processing and storage facilities located in close proximity to any hazard processes, activities, or storage? • Could a loss event in these areas compromise or spread to data processing and storage facilities?		
12.	• Have all data processing and storage facilities been designed to provide adequate redundancy for all critical components or equipment including cooling systems? • Are any back up or duplicate systems routinely tested?		
13.	• Have all data processing and storage facilities been designed to provide suitable processing capacity to avoid overworking and stressing critical components?		
14.	• Have data processing and storage facility cooling systems been designed and the cooling requirements, calculated by a competent person or firm? • Have cooling systems been assessed by the installers of any fire detection and fire protections to ensure air movements within the data processing/storage facilities do not impact performance of the fire systems? • Are temperature monitoring systems installed that provide adequate alarm warning of overheating issues?		
15.	Has fire resistant and fire retardant cabling been utilised where possible?		
16.	Have service maintenance arrangements been established for significant equipment within server/comms rooms including cooling, ventilation, electrical installations, fire detection and fire protections?		

LOSS PREVENTION STANDARDS

17.	• Has the facility been assessed for the presence of any wet services that might lead to damage in the event of water or fluid leaks? • Has this been extended to cover the risk of liquid escape from cooling system condensate and return cycles? • Are any bathrooms, wet rooms or water storage vessels located in close enough proximity to cause damage to server/comms rooms in the event of escape, leaks, or overflowing? • If yes, have these rooms been tanked to prevent water egress? • Are any server/comms rooms exposed to water ingress attributed to blocked and overflowing guttering systems? • If yes, could these guttering systems be relocated? • If no, procedures in place to undertake guttering checks undertaken?		
18.	• Have fire detection and protection systems been designed by an accredited company? • Have design specifications been reviewed and approved by Insurers? • Are interlocks subject to at least annual testing? • Are alarm monitoring systems fully operational?		
19.	• Has a security assessment been completed by a competent person? • Are the doors to server/comms rooms fitted with good quality locking devices? • Are any accessible windows fitted with good quality window locks? • Are any additional window security measures required, such as collapsible security shuttering, fixed security grilles, internal security barring? • Do any high value components require individual security protection e.g., security cages or security cables affixed to a solid wall or floor. • Are there processes in place to change access codes upon authorised persons leaving the business, no longer requiring access to the facility etc?		

LOSS PREVENTION STANDARDS

	Housekeeping and Self Inspections	Y/N	Comments
20.	• Are formal housekeeping standards in place? • Is the storage of spares, filing, furniture and combustible goods prohibited within server/comms rooms? • Are nominated persons responsible for organising cleaning and reviewing housekeeping standards? • Is regular deep cleaning undertaken to remove dust accumulations?		
21.	• Are server/comms rooms subject to weekly inspections checking for: 　▪ Physical damage to the room or equipment including cooling plant? 　▪ Overheating components? 　▪ Loose or damaged cabling? 　▪ Impaired fire detection or fire protection systems/components including integrity seals? 　▪ Housekeeping issues? 　▪ Evidence of water ingress or other fluid related issues? 　▪ Security breaches or concerns? 　▪ Faults or issues with ventilation systems?		
22.	Are self-inspection checklists routinely audited to ensure they are being completed accurately and at the agreed timescales?		

	Scheduled Inspection Checklist	Y/N	Comments
23.	• Are server/comms rooms adequately secured? • Are there any signs of attempted ingress? • Are locking devices working normally? • Are any window shutters or grilles in normal working order?		
24.	• Are any intruder alarm protections working normally? • Is any intruder alarm monitoring routinely tested with the Alarm Receiving Centre? • Are any Video Surveillance Systems working normally? • Are cameras obscured or covered?		
25.	• Is there any evidence of physical damage to the room including doors, seals, self-closing devices? • Are all ceiling panels in place? • If no to any of the above, have repairs been instigated or completed?		

LOSS PREVENTION STANDARDS

26.	• Is there any unapproved storage within any server/comms rooms?		
27.	• Are any lithium-ion batteries in UPS and BBU systems in good order with no signs of damage e.g., cracking/damage to housing, leaks, unusual odours etc? • Are UPS/BBU adequately cooled?		
28.	• Are there any signs of water or other fluid ingress? • Any staining to ceiling or walls indicating a water or fluid related issue? • Where present, are leak detection systems functioning normally including alarms?		
29.	• Are any intruder alarm protections working normally? • Is any intruder alarm monitoring routinely tested with the Alarm Receiving Centre? • Are any Video Surveillance Systems working normally. • Are cameras obscured or covered?		
30.	Are ventilation systems operating normally?		
31.	• Are automatic fire detection and any automatic fire protection systems such as gaseous fire suppression systems in normal working order? • Are pressure gauges on gaseous fire suppression cylinders working normally? • Are there any pressure related issues? • Are there any keys in control panels?		
32.	Are alarm monitoring systems in normal working order?		
33.	• Are interlocks in place and fully functioning? • Are interlocks tested at least annually?		

LOSS PREVENTION STANDARDS

30th September 2024

Version 1.0

URN - ARMSGI2082024

LOSS PREVENTION STANDARDS