CSH

MINISTRY OF SECURITY

Data Center Security Checklist

Personnel and Process Management

S.No	Guidance	Compliance
1	Is there a Data Center organizational chart with organizational structure and job descriptions.	
2	Do each staff member have documented job descriptions?	
3	Are the personnel in the data center aware of their job functions?	
4	Are the risks associated with data center processes identified and controls are implemented?	

Organization and Management

S.No	Guidance	Compliance
1	Is there a standard data center operating policy and guidance?	
2	Is the data center operating policy and guidance approved by senior management?	
3	Is the operating policy descriptive enough to guide the management and operation of the data center?	
4	Are the data center operators aware of the existence of the user manual?	
5	Is there a mechanism for reviewing the operating manual regularly to reflect changes and improvements in data center operations and to verify that best practices are followed?	
6	Is an operator logbook maintained to capture critical events and corrective actions in the data center?	
7	Do each duty shift in the data center have a handover report written on the completion of their shift on activities performed and key issues to assist with smooth takeover until the next shift?	
8	Are all End of Day (EOD) or End of Month (EOM) events and processes to prevent system breaches, suppression of malicious acts, or service failures tracked?	
9	Are the EOD/EOM activities and processes regularly reviewed to ensure no service issues or malicious acts are overlooked?	
10	Are the incidents recorded during EOD/EOM processing promptly forwarded to relevant administrative persons for resolution?	

Capacity Utilization

S.No	Guidance	Compliance
1	Is the capacity management and planning measures identified and documented?	
2	Is the resource monitoring software installed to monitor the capacity usage of resources on all relevant servers, especially critical systems and applications?	
3	Are system resource usage reports regularly reviewed?	
4	Are the times of peak resource demand during the processing day identified?	
5	Does the IT management receives feedback on system capacity usage reports to plan future server or application acquisition as part of their strategic function?	

Performance Management

S.No	Guidance	Compliance
1	Are the performance measurement and monitoring systems identified and documented?	
2	Are the performance measurement process services and infrastructure in place?	
3	Is the system outage is recorded or monitored?	
4	Are the alerts and notifications set to follow agreed resource thresholds so that systems trigger or alert Operators when set points are violated or exceeded?	
5	Is the system downtime or outage being actively monitored to prevent service failure?	

Backup Environment and Management

S.No	Guidance	Compliance
1	Are adequate controls to ensure accountability and protection of backup media produced at the main site and their transfer and retrieval to the offsite storage facility sufficient?	
2	Are all tapes sent to the offsite storage facility appropriately documented and authorized before transfer?	
3	Is the method of transferring tapes to the offsite storage facility, secure and adequately protected against theft or danger?	

4	Is the box or case and the tape transfer process to ensure the safety of the tapes examined?	
5	Verify that tapes and other media are encrypted to prevent them from being accessed or compromised in the event of theft or loss.	
6	Verify that the default encryption code has been changed and is not used to encrypt tape drives during backup.	
7	Are all visitors to the offsite facility required to sign a logbook stating their name, the reason for visit, time and date, or record their presence?	
8	Are recovery processes of storage media (tape and hard drives) documented and adequately controlled to ensure that the correct tapes are retrieved, and appropriate entitlements are available?	
9	Is storage media (tapes and hard drives) correctly indexed and labelled to facilitate easy storage and retrieval?	

Environmental Control and Monitoring Systems

S.No	Guidance	Compliance
1	Is the data center operators and other personnel on-site are adequately trained on how to respond in the event of a fire?	
2	Are the data center operators adequately trained to do different fire emergencies or security breaches occur?	
3	Are other personnel in the facility sufficiently responsive to what to do when fire emergencies occur?	
4	Are only the authorized persons assigned to critical areas of the facility and are adequately equipped with essential tools to coordinate emergency evacuation activities?	
5	Are frequent fire drills are conducted to create the necessary awareness of all employees to respond adequately to emergency or fire incidents?	
6	Are fire equipment and other emergency controls installed is adequately maintained and tested to respond to any fire exits?	
7	Are fire alarm pull boxes and emergency power switches visible, marked and unobstructed?	
8	Are there clear and adequate fire instructions at all locations in and around the data center?	
9	Are the emergency phone numbers for fire officials prominently placed around the facility for easy access and usage in the case of a fire.	
10	Are smoke and heat detectors periodically tested to determine operating conditions and their ability to detect the presence of fire or smoke when needed?	
11	Are smoke detectors strategically placed under raised floors and on the data center ceiling to easily detect smoke or fire?	

12	Are there enough fire alarm pull boxes in and around the data center?	
13	Are operators given individual responsibilities in case of fire?	
14	Are operators trained on firefighting periodically?	
15	How often are fire drills held?	
16	Are FM200 fire extinguishers installed in the data center for firefighting?	
17	Are FM200 extinguishers maintained and serviced by their service lifecycle?	
18	Is firefighting equipment periodically tested to determine its operational status and ability to respond to a disaster in an emergency?	
19	Are there flammable materials in and around the data center area?	
20	Ensure controls to adequately prevent floods and other disasters from affecting the data center.	
21	Is the data center built on a raised floor?	
22	Are the materials used for the raised floor or floor of the data center non-combustible or non-conducive to the fire spread?	
23	Are there water lines or pipes running through or near the data center area to prevent flooding?	
24	Is there an environmental monitoring and control system (EMCS) installed in the data center to ensure that the data center's temperature and humidity levels are managed and monitored?	
25	Is the data center environmental monitoring and control system (EMCS) periodically tested?	
26	Are the EMCS configurations adequate to ensure that triggers or alerts are sent to the appropriate individuals when temperature and humidity conditions within the data center fall or rise above acceptable limits or thresholds?	
27	Is the main wiring and cabling system in and around the data center implemented to prevent physical damage?	
28	Check to make sure electrical power cords and cables around the data center are well organized in enclosures to prevent physical damage.	
29	Does the data center have a redundant cooling system?	
30	Is there a UPS system to back up the data center electricity?	
31	What is the backup capacity of the UPS System and when was it last tested?	
32	Inspect all signal and data cables on servers and network devices to ensure they are not subject to interference or touch.	

Physical Access Controls

S.No	Guidance	Compliance
1	Is there a biometric or smart card access control device to restrict access to the data center?	
2	Is there a process to grant users access to the data center?	
3	Do all personnel enter the data center enter from an entry point controlled by a biometric or smart card access control device that the Data Center Manager monitors?	
4	Is there a procedure for reviewing biometric or smart card activity logs?	
5	Are the log reviews performed by an authorized person?	
6	Do biometric or smart card devices restrict access based on an individual’s unique access credentials?	
7	Do biometric or smart card devices restrict access to designated doors for users or at a particular time of day?	
8	Are biometric or smart card access methods challenging to replicate or compromise?	
9	Is there a process for disabling access of biometric or smart card devices of the users leaving the organization?	
10	Do access devices such as biometrics or smart cards automatically generate a silent or audible alarm when attempting unauthorized access?	
11	Do biometric or smart card devices automatically record and report successful data center access and failed attempts?	
12	Is it a carefully controlled administrative process of the smart card or biometric card’s issuance, accounting, and recovery?	
13	Are the access logs of biometric or smart card devices retained for a reasonable period?	
14	Are the logs backed up to external media to be retained for research purposes as needed.	
15	Are there video cameras monitored by security personnel at strategic points in the data center?	
16	Is video surveillance recorded for possible future checks?	

17	Is there an alarm system connected to inactive entry points to the data center?	
18	Are employees and visitors required to wear a photo ID card?	
19	Do all visitors have to sign a visitor diary stating their name, companies represented, reasons for visiting, and people to see before accessing the data center?	
20	Do visitors need to provide a method to authenticate before gaining access?	
21	Do visitors need to wear a different colour ID card than the employee badge for easy identification?	
22	Are visitors/guests escorted inside the premises?	
23	Are personnel with special service contracts, such as cleaning personnel, monitored during the performance of their duties?	

Inventory Management

S.No	Guidance	Compliance
1	Is an inventory of the assets in the data center maintained up to date?	
2	Is the asset inventory in the data center reviewed?	
3	Are all assets in the data center adequately labelled?	
4	Does the vendor have contact information for the relevant systems in the data center in an emergency?	

Incident Management

S.No	Guidance	Compliance
1	Does the Data Center have an Incident Management policy?	
2	What methodologies are adopted for Incident Management?	
3	Have management roles and processes been developed to guarantee that information security events are handled quickly, effectively, and orderly?	
4	Have roles and responsibilities been defined for incident management?	
5	Are incidents documented and reported?	
6	Is root cause analysis performed to prevent incidents from occurring?	
7	Are emergency plans in place?	

Disaster Recovery and Business Continuity Management

S.No	Guidance	Compliance
1	Is there a disaster recovery plan?	
2	Are all processes documented in the case of Disaster Recovery?	
3	Does the Disaster Recovery policy specify roles and responsibilities for planning, testing, oversight management, and accountability?	
4	How often is the Disaster Recovery site tested?	
5	Are disaster recovery test reports approved by the relevant administrator?	

Reference: ISO 27001, PCI DSS v3.2.1 etc.