HITRUST

Possible Alternate Implementation Validation Procedures to Level 1, 2, and 3 CSF Requirements Typically Tested through Observation

HITRUST CSF Requirement Statement	Possible Alternate Implementation Validation Procedures
1815.08d2Organizational.123: Fire prevention and suppression mechanisms, including workforce training, are provided.	Inspect documentation reflecting the existence of and placement location of fire suppression equipment, potentially including: ○ Facility placement diagrams ○ Fire suppression system maintenance records ○ Service tickets from initial fire suppression system installations ○ Post-installation inspection reports ○ Fire Chief inspection reports
0503.09m1Organizational.6: Wireless access points are placed in secure locations.	Inspect documentation reflecting the secure placement/location of wireless access points, potentially including: ○ Facility wiring diagrams ○ Facility diagrams ○ Service tickets from initial installation and/or ongoing maintenance of WAPs which may describe placement location ○ Screenshots of camera feeds ○ Badge and/or card reader access history ○ Badge and/or card reader access reports
1114.01h1Organizational.123: Covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors.	Inspect documentation generated by management through procedures performed by management to monitor for consistent observance and enforcement of clean desk, clean screen, and clean printer requirements, potentially including: ○ Populated periodic clean-desk walkthrough checklists ○ Reports from sanctioning personnel for failing to observe these requirements
1192.01l1Organizational.1: Access to network equipment is physically protected.	Inspect documentation evidencing the location of on-premise networking equipment and the physical protections in place for these locations, potentially including: ○ Facility wiring diagrams ○ Facility diagrams ○ Camera footage ○ Service tickets from initial installation and/or ongoing maintenance of networking equipment installations which may describe placement location ○ Service tickets from initial physical security equipment installations which may describe placement location ○ Facility floor plans / diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) ○ Badge and/or card reader access history ○ Badge and/or card reader access reports

HITRUST

HITRUST CSF Requirement Statement	Possible Alternate Implementation Validation Procedures
1801.08b1Organizational.124: Visitor and third-party support access is recorded and supervised unless previously approved.	Inspect documentation evidencing the protections observed for site visitations, potentially including: ○ Camera footage ○ Logs from visitor check-in / check-out systems ○ Service tickets from initial installation and ongoing maintenance of visitor badge printers ○ Scans of hard-copy visitor check-in / check-out logs ○ Reports from sanctioning personnel for failing to properly record and supervise visitors
1802.08b1Organizational.3: Areas where sensitive information (e.g., covered information, payment card data) is stored or processed are controlled and restricted to authorized individuals only.	Inspect documentation evidencing the physical protections in place for areas where sensitive information is stored or processed, potentially including: ○ Camera footage ○ Service tickets from initial installation and/or ongoing maintenance of physical security systems ○ Facility floor plans / diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) ○ Badge and/or card reader access history ○ Badge and/or card reader access reports ○ Logs of alerts generated by the physical security system such as forced entry alerts, door held open alerts, etc. ○ Logs generated by rounds performed by guards or Floor Marshalls
1845.08b1Organizational.7: For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points, maintains physical access audit logs, and provides security safeguards that the organization determines necessary for areas officially designated as publicly accessible.	Inspect documentation evidencing the physical protections in place for areas where information systems reside, potentially including: ○ Camera footage ○ Service tickets from initial installation and/or ongoing maintenance of physical security systems ○ Facility floor plans / diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) ○ Badge and/or card reader access history ○ Badge and/or card reader access reports ○ Logs of alerts generated by the physical security system such as forced entry alerts, door held open alerts, etc. ○ Logs generated by rounds performed by guards or Floor Marshalls
1814.08d1Organizational.12: Fire extinguishers and detectors are installed according to applicable laws and regulations.	Inspect documentation reflecting the existence of and placement location of fire detection and suppression equipment, potentially including: ○ Facility placement diagrams ○ Fire detection and suppression system maintenance records ○ Service tickets from initial fire detection and suppression system installations ○ Post-installation inspection reports ○ Fire Chief inspection reports

HITRUST CSF Requirement Statement	Possible Alternate Implementation Validation Procedures
18127.08l1Organizational.3: Surplus equipment is stored securely while not in use and disposed of or sanitized when no longer required.	Inspect documentation evidencing the physical protections in place for areas where surplus equipment is stored while not in use, potentially including: o Camera footage o Service tickets from initial installation and/or ongoing maintenance of physical security systems o Facility floor plans / diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) o Badge and/or card reader access history o Badge and/or card reader access reports o Logs of alerts generated by the physical security system such as forced entry alerts, door held open alerts, etc. o Logs generated by rounds performed by guards or Floor Marshalls o Asset inventories reflecting the physical location of surplus equipment
1817.08d3Organizational.12: Water detection mechanisms are in place with master shutoff or isolation valves accessible, working, and known.	Inspect documentation reflecting the existence and placement location of water detection and control mechanisms, potentially including: o Service tickets from initial installation and/or ongoing maintenance of water detection and control mechanisms o Post-installation inspection reports