**ITD\_0091A Secure Areas Policy Summary**

**Contractors and Vendors**

1. **PURPOSE:**

The purpose of this policy is to ensure the protection of HHSC Information Assets by providing the appropriate physical security and environmental controls to prevent unauthorized physical access, damage, interference, or other activities compromising the security, availability, and integrity of HHSC Information Assets. Information Assets include all resources such as data centers, communications rooms, databases and other data repositories, servers, workstations, handheld computing devices, networking infrastructure, routers and other communications hardware, disk drives, etc that form a system that is used to maintain and process information necessary to allow HHSC to perform its mission.

1. **DEFINITIONS:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Secure Areas | Areas or facilities that are deemed to house critical infrastructure components supporting HHSC Information Assets |
| Sensitive Information | Refers to information that is classified as Internal Use Only, Confidential, or Confidential-Reportable as defined in Information Classification Policy. |
| Stakeholder | Any person who uses HHSC Information Assets, including, but not limited to HHSC facility and corporate office employees, board members, volunteers, students, physicians, vendors, contractors, and other external parties. |
| Tier Standards | A four-tier system that provides a simple and effective means for identifying different data center site infrastructure design topologies. The Uptime Institute's tiered classification system is an industry standard approach to site infrastructure functionality addressing common standard needs. |

III. **POLICY:**

**1. Physical Security Perimeter**

**1.1. Office Areas**

Areas where stakeholders work with HHSC Information Assets must be protected with physical security measures that minimize the risk of adverse impacts to the security, availability or integrity of HHSC Information Assets.

Stakeholders must ensure that their work area is secured from unauthorized access to Confidential, or other Sensitive Information and must take steps to ensure the protection of such information when leaving their area for any extended period of time.

**1.2. Patient Care Areas**

Workstations, printers, and other HHSC Information Assets in patient care areas must be protected with physical security measures that minimize the risk of unauthorized disclosure of Sensitive Information. These measures may include but are not limited to:

* Physical placement of workstations and printers to minimize the ability of visitors, patients and other non-authorized persons to see Sensitive Information on the workstation screen or printer output.
* Privacy screens on monitors
* Restricted access (i.e. operating room suites, radiology reading rooms and other areas where access is tightly controlled).
* Inactivity timeouts, screen savers and other means to remove Sensitive Information from computer monitors.
* Shredders or shred-bins for the disposal of paper containing Sensitive Information.

**1.3. Critical Infrastructure Areas**

The Chief Information Security Officer (CISO) must maintain an inventory of all facilities or areas that are deemed to house critical infrastructure components supporting HHSC Information Assets and designate them as Secure Areas. These include data centers, major communication rooms, and telephone node rooms.

Primary data centers must be constructed to meet or exceed Tier 3 standards (as defined by the Uptime Institute) where feasible and secondary data centers must be constructed to meet Tier 3 standards.

Other Secure Areas must be constructed to ensure access is restricted to authorized personnel and the appropriate environmental controls are in place to ensure the correct operation of the equipment.

Each Secure Area must have a physical security plan and procedures that are reviewed and updated periodically by the Manager in charge of the facility. There may be areas where it is not technically or economically feasible to apply strict access controls or the risk may not warrant them. In that case, the plan must detail the risk and mitigating factors. This plan and procedures must also be reviewed and approved by Chief Information Security Officer (CISO).

There must be no signage indicating the location or function of a data center, communication room or any other Secure Area.

**2. Physical Entry Controls**

**2.1. Physical Access Control to HHSC Information Assets**

Except for public areas such as lobbies where visitor or guest access is allowed for business reasons, access to any work area containing HHSC Information Assets must be physically restricted to limit access to those with a legitimate reason to be there.

**2.2. Identification Badges**

The Manager of each Secure Area is responsible for developing procedures to ensure that the entry and departure of each individual is recorded, each individual can be readily identified, and each individual's purpose for entering the area is known. At a minimum, the procedures should ensure that:

* All personnel entering HHSC Secure Areas must display a picture identification badge and their entry and departure shall be logged.
* External parties who do not have a permanent HHSC picture identification badge shall be required to state the purpose for their entry, and their activities will be monitored.
* Individuals without a clearly visible identification badge must be escorted out of the area if they cannot produce a valid badge.
* Access records must be retained for at least one year.

**2.3. Bag Inspection**

All briefcases, suitcases, handbags, and other luggage may be subject to inspection when people leave the Secure Area.

**2.4. Physical Access of Terminated Stakeholders**

When a stakeholder terminates a business relationship with HHSC, all badges, security access cards and keys must be retrieved, deactivated, or changed as required by Termination or Change of Employment Policy and the HHSC Human Resources Guidelines.

**2.5. Authorized Physical Access List**

A list of Managers who are authorized to grant access to HHSC Secure Areas must be kept up to date and periodically reviewed by the CISO.

An Authorized Physical Access List of all stakeholders who are currently authorized to access a Secure Area must be maintained, reviewed, and updated by the Manager responsible for that area.

**2.6. Tours of Secure Areas**

Tour of HHSC Secure Areas must be authorized in advance by the appropriate Manager and the CISO.

**3. Working in Secure Areas**

**3.1. Staffing Requirements**

All Secure Areas must be monitored at all times by technically-proficient staff 24 hours a day, seven days a week, 365 days a year to ensure that all of the hardware, software, UPS, power, cooling, and other components are functioning correctly.

**3.2. Audio or Video Recording Equipment**

Cameras, audio recording equipment, and video recording equipment must not be used within Secure Areas without written prior authorization by the facility Manager and the Chief Information Officer (CIO) or CISO.

**3.3. Isolated Delivery and Loading Areas**

A secured and separate holding area must be used for computer supplies, equipment, and other deliveries to ensure that deliveries are not made directly to the Secure Area.

1. **APPLICABILITY:**

This policy applies to all HHSC facilities and HHSC Corporate Office stakeholders responsible for information processing facilities and other areas housing HHSC Information Assets. Compliance with this policy is mandatory. Compliance will include periodic reviews by the HHSC Information Security Team. Information Security Policy Exception Requests must be submitted in writing by relevant Management to the Chief Information Security Officer (CISO), who will facilitate HHSC Leadership approval. Requests shall include justification and benefits attributed to such exception.

1. **REFERENCES:**

* ISO/IEC 27002:2005, an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology - Security techniques - Code of practice for information security management:

o Section 9: Physical and Environmental Security Management Objectives

* 9.1 Use secure areas to protect facilities
* Security Standards for the Protection of Electronic Protected Health Information 45 CFR Part 164 Subpart C; 45 CFR 164.310(a)(i); 45 CFR 164.310(a)(2)(ii)