HARRIS COMPUTER SYSTEMS

CORPORATE FACILITY ACCESS CONTROLS POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: ______________________________

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/22/16	Gina Martin/Katie Rose	Major	Initial version of policy.	Todd Richardson
1.1	10/22/18	Katie Rose	Minor	Annual Review	Dwayne Martin
1.2	3/25/2020	Katie Rose	Minor	Annual Review, Inserted requirement for key card or other physical security control	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Edits to incorporate controls from USHC Policy as appropriate	Dwayne Martin

POLICY

The purpose of this policy is to allow Harris Computer Systems (Harris or Company) to protect the confidentiality, integrity, and availability of its information systems by preventing unauthorized physical access, tampering, and theft to the systems and to the facilities in which they are located, while ensuring that properly authorized access is allowed and to be compliant as a Business Associate of Covered Entities where appropriate and applicable.

SCOPE

1. This policy applies to all of Harris.

2. This policy describes the Company's objectives and policies regarding maintaining the security of Harris' systems and data.

PROCEDURE

1. Harris' Executive Vice Presidents or their designees on an annual basis will review and attest to the implementation of this policy as appropriate for their business. Harris' Executive Vice President may designate a facility manager to implement the requirements of this policy, or all Harris Executive Vice Presidents may designate one facilities manager to implement the requirements of this policy.

2. Harris' information systems are physically located in areas where unauthorized access is prevented. Harris ensures the level of protection provided for the Company's information systems and the data stored on them are appropriate with that of the identified risks and the level of criticality of assets and the classification of the data.

3. Harris performs an annual inventory of all physical access controls used to protect information systems at its facilities and an assessment of the risks to such facilities and information systems containing ePHI, PII or other Sensitive Information. The inventory report and assessment are stored in a secure manner.

4. The perimeter of a building or site containing Harris' information systems is physically sound; the external walls of the site are solidly constructed and all external doors have appropriate protections against unauthorized access.

5. Physical barriers are extended from actual floor to actual ceiling to prevent unauthorized entry. Doors and windows are locked when unattended. Intrusion detections systems such as alarms are installed on all accessible doors and windows where appropriate. Key card access or other physical authentication controls are

used to access facilities as appropriate. Key cards or other physical authentication controls are changed or revoked when lost, stolen, compromised or when a user's access requirements changes. Facilities are accessible after hours by individually issued key card access only.

6. Delivery and loading areas are controlled to prevent unauthorized access.

7. All physical access rights of all employees, contractors, visitors and probationary employees to areas where information systems are maintained are regularly reviewed and revised as necessary.

8. All authorized visitors must show proper identification and sign a log to indicate date of access, time of entry and reason for the visit prior to gaining physical access to areas where Harris' information systems are located. Visitors are required to sign out when leaving the area and are escorted at all times. Logs are regularly reviewed and maintained as appropriate.

9. In the event of an emergency or disaster and in support of restoration of lost data, only authorized Harris users may administer or modify processes and controls on information systems and data.

10. Harris implements appropriate safeguards for the environmental and physical protection of all equipment including but not limited to temperature controls, redundant power supplies, fire prevention, detection and suppression and access restrictions. Such equipment includes, but is not limited to workstations, servers, removable devices, tablets, laptops.

11. The Company documents all repairs and modifications to the physical components of its facilities where information systems are maintained that are related to facility security.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

45 C.F.R. 164.310(a)(1)