HARRIS COMPUTER SYSTEMS

CORPORATE ASSET TRACKING POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: _____

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/08/16	Gina Martin/Katie Rose	Major	Initial version of policy.	Todd Richardson
1.1	10/22/2018	Katie Rose	Minor	Annual Review	Dwayne Martin
1.2	3/25/2020	Katie Rose	Minor	Annual Review, inserted policy review information, clarified asset classification and added asset inventory statement	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document, Edits to incorporate controls from USHC Policy as appropriate	Dwayne Martin

PURPOSE

Adherence to this policy enables Harris Computer Systems (Harris or Company) to track assets by their location and by who is using them. This information is critical to have on hand in the event a device containing Protected Health Information (PHI), Personally Identifiable Information (PII) and other Sensitive Information is breached, lost or stolen. This policy supplements the Corporate Back-Up, Device and Media Controls Policy and the Corporate Portable Computing Devices Policy.

POLICY

Harris is committed to maintaining the security of, PHI, PII and other Sensitive Information and the Harris assets by implementing the following policy to help track and prevent the loss of information by tracking the Harris assets. This policy and supporting asset tracking processes are reviewed periodically and updated as appropriate.

PROCEDURE

1. Types of Assets to Track. Corporate IT tracks the following Corporate IT supported and managed assets (owned or leased):

    Desktop workstations

    Laptop computers

    Servers

    Network Devices

    Scanners, copy machines, printers and fax machines

    Handheld devices, including iPhones, iPads, Droids, other smart phones or tablets, and smart watches

    Memory devices, including jump or thumb drives and portable hard drives and on any other hardware that may store PHI, PII or Sensitive Information if any are provided.

2. Asset Tracking Database. Corporate IT maintains the Asset Tracking Database that tracks the following information for each device listed above and other information as appropriate for each asset:

    Serial number

    Asset Type and Brand

    Current Location

    Designated employee

    Access to PHI, PII and other Sensitive Information is classified accordingly

    Password protection installation

When the device has been encrypted

3.   Adding Assets to the Asset Tracking Database

When the Company acquires a new asset, it will be added to the Asset Tracking Database before assigning the asset to an employee or Workforce Member.   Devices, with the exception of scanners, copiers and fax machines, will not be distributed to employees until they are password protected. Persons responsible for newly purchased or leased copiers, faxes or scanners will notify Corporate IT when these types of devices are acquired to ensure they are secured appropriately for data protection. Persons responsible for retiring or returning copiers, faxes or scanners will notify Corporate IT prior to retiring, destroying, returning or reissuing these devices for proper data sanitation.

4.   Updating the Asset Tracking Database

Whenever a tracked asset is transferred to a different employee or moved to a new location, Corporate IT will be notified and will update the information in the Asset Tracking Database as soon as possible. If an asset is disposed of, the asset will remain in the Asset Tracking Database with a location of "destroyed" or "purged". Any reuse or disposal of any asset is conducted in accord with the Corporate Back-Up, Device and Media Controls Policy. Reconciliation of assets is done periodically to ensure the items in inventory align with the physical assets, duplications are not present, no unauthorized assets are present, and controls are appropriate for the asset classification.

5.   Lost or Stolen Assets

All employees are required to notify Corporate IT and the Security Officer immediately upon discovering an asset has been lost or stolen. Whenever a Company asset is lost or stolen, the designated employee must follow the Portable Computing Device Policy. Corporate IT will update the asset's location in the Asset Tracking Database as "Lost or Stolen." Refer to Data Incident Policy.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

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