

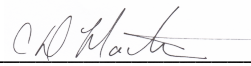


HARRIS

HARRIS COMPUTER SYSTEMS

CORPORATE BACKUP, DEVICE AND MEDIA CONTROLS 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, Revised title of this policy to reflect backups.	Dwayne Martin
1.2	3/25/2020	Katie Rose	Minor	Annual Review	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

POLICY

Harris Computer Systems (Harris or Company) will ensure that computer equipment and electronic storage media that contain Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information has appropriate safeguards, is regularly monitored and the information is disposed of in a secure manner to avoid any inadvertent disclosure of any PHI, PII or other Sensitive Information. Backup copies of information and software are made, and tests of the media and restoration procedures are regularly performed at appropriate intervals. All PHI, PII or other Sensitive Information is

backed up in encrypted format to ensure confidentiality. Controls are maintained for all hardware and software moving into, out of and within the Harris facilities.

Harris will maintain, in conjunction with the Asset Tracking Policy a policy for the receipt and removal of all hardware and software, including any contained within electronic storage media. Electronic storage media includes, but is not limited to, magnetic tapes, CDs, DVDs, hard disk drives, laptops, copy machines, smart phones, USB/thumb drives or other similar devices used to electronically store data. This policy includes both portable and non-portable devices.

SCOPE:

- a. This policy applies to all Harris employees, management, contractors, vendors, student interns, and volunteers.
- b. This policy describes Harris' objectives and policies regarding maintaining the security of PHI, PII or other Sensitive Information.
- c. The Company desires to be compliant as a Business Associate of Covered Entities as appropriate.

PROCEDURE

- 1) Data Backup and Storage. All Company back up data is retained in accordance with the Document Retention and Storage policy and procedure as required by applicable laws and regulations. This excludes any data that is hosted on behalf of a third party.
 - a) All backup media will be maintained by vendors and destroyed in accordance with this policy. Vendors engaged for the purposes of destruction of backup media will be required by contract to ensure destruction in accordance with relevant regulatory compliant methodologies.
 - b) All media is governed and managed by the following policy provisions.
 - i) CD's and other portable media storage devices only have the necessary data for someone to perform their job function. PHI, PII and other Sensitive Information will not be stored on portable devices.
 - ii) All portable media storage devices are physically secured by the individual using them and are destroyed in a manner appropriate for the data retained and in a timely fashion.
 - iii) Any data electronically transmitted to off-site locations utilizes secure communication protocols, such as SSL and other forms of data encryption.
 - iv) Third party vendors maintaining Company data are not permitted to use or disclose it unless specified in contracts with the third-party vendors. The

contract provisions with third party vendors contain provisions around securing the data and its use. If the Third-party vendor is maintaining PHI, the contract with the vendor must include a subcontractor Business Associate Agreement.

- v) The creation of backup jobs, job scheduling, and job processing are the responsibility of designated Harris application owners or CIT where appropriate.
 - vi) Where possible, automated software is used to schedule, process and track: data backups, backup media used to retain the data and the physical location of the media. Data backup failures are reported to the Information Owner and actioned by the Information Owner or application owner as appropriate in a timely manner. When automated solutions are not available, the Corporate IT Leader or the Company designee will maintain a log sheet of all backup media, its contents, and physical location.
 - vii) All backup media is maintained and stored in a secure data center until it is transferred to a secure off-site location.
 - viii) The Corporate IT Leader or their designees are the only individuals who can authorize the movement of backup media to a location other than the data center.
 - ix) All Company data is considered business confidential.
- c) Offsite storage is governed and managed by the following policy provisions
- i) Backups are stored in a physically secure remote location with appropriate environmental controls, at a sufficient distance to make them reasonably immune from the same conditions which may cause damage to data at the primary site
 - ii) The Corporate IT Leader or their designees are the only individuals who can authorize the movement of backup media to and from the off-site location.
 - iii) All media transferred to off-site locations is placed in secure containers identified by media labels indicating the contents are the Harris' Confidential Materials.
 - iv) Only Harris authorized personnel, or the off-site storage vendor are allowed to transport the media to and from the off-site location

- v) All backup media stored off-site is inventoried by Harris and the vendor.
 - vi) Vendors providing off-site storage of electronic media shall maintain sufficient controls so that all Harris media is secure with the appropriate physical and environmental safeguards. Access to the media is only granted to those individuals identified by the Security Officer, or their designees. Where possible, these provisions are included in the contracts with the vendor.
 - vii) The Company will perform an annual assessment of any vendors providing off-site storage services. At a minimum, the assessment includes the positive confirmation the vendor maintains sufficient physical and environmental controls to protect Harris media. Any potential weaknesses are brought to the vendor's attention and corrective action is pursued. An SSAE 16 report over the controls of the vendor shall be requested and reviewed.
 - viii) Harris will perform an annual assessment to confirm Harris' off-site inventory listing reconciles to the media possessed by any vendors. Any discrepancies are investigated, and corrective action is pursued.
- 2) Accountability. Harris maintains an asset tracking system to record the movements of all hardware and electronic media owned and leased by the Company. (See Asset Tracking Policy). The tracking system is intended to assist the Security Officer in making sure no PHI, PII or other Sensitive Information is inadvertently accessed, released or shared with an unauthorized person. Appropriate verification for the removal or destruction of devices containing PHI, PII or other Sensitive Information will be obtained.
- 3) Media Reuse. Prior to making the determination whether to reuse or dispose of the electronic storage media, all PHI, PII or other Sensitive Information shall be identified. In limited situations electronic storage media may be reused, however all reuse must be properly documented and free from any PHI, PII or other Sensitive Information prior to the reuse.
- a) Equipment recognized as having nominal or no value may be salvaged. Only approved salvage vendors are used. Vendors must meet legislative requirements as outlined by Fair and Accurate Credit and Transaction Act (FACTA) and meet applicable EPA requirements and also have the capability to meet the US Department of Defense 5220.22-M Standards for data sanitization. Harris requires certificates of sanitization, or physical destruction of any hard drives that are sent for salvage. Typically, the Company will physically remove and destroy PC/Laptop hard drives before salvaging the PC or Laptop. Harris does not salvage servers or their drives

- i) All transactions that include return to lesser, salvage, or sell will be forwarded to Asset Management.
 - ii) Asset Management will create a record with the aforementioned information.
 - iii) Asset Management will provide monthly and year-to-date reporting of all these records.
- 4) Disposal. All Harris workstations, laptops, and Intel-based servers to be disposed of are sanitized using a triple-pass overwrite procedure. (Whenever possible, the overwrite procedure shall be modeled after the U.S. Department of Defense 5220.22-M Standards.)
- a. All of Harris electronic storage media that is not reused must be destroyed after its use. The destruction must be done in accordance with the instructions outlined by the Security Officer and coordinated with vendors to ensure that no PHI, PII or other Sensitive Information is compromised. Such vendor shall be a Business Associate where applicable.
 - b. Any device or drive that fails to wipe clean is fully destroyed.
 - c. Equipment recognized as having value may be sold. In these cases, hard drives will be sanitized using a triple-pass overwrite procedure modeled after US Department of Defense 5220.22-M Standards or destroyed (physically or by degaussing) prior to their sale.
 - d. All backup media will be maintained by vendors and destroyed in accordance with Harris' Policy and Procedure. Vendors engaged for the purposes of destruction of backup media shall be Business Associates and required by contract to ensure destruction in accordance with relevant regulatory compliant methodologies where applicable.
 - e. Prior to returning any leased equipment, including any copier machines, fax machines or scanners, the data on the hard drives shall be downloaded for retention and any PHI, PII or other Sensitive Information that may be retained on the hard drives will be sanitized prior to return.

DEFINITION

See attached policy definitions or [click here](#).

REGULATORY REFERENCES

45 C.F.R. § 164.310(d)

U.S. Department of Defense 5220.22-M Standards
NIST 800-53 Revision 5 MP1-6

Harris Computer Systems
Corporate Backup, Device and Media Controls

