



HARRIS

HARRIS COMPUTER SYSTEMS

CORPORATE PORTABLE COMPUTING DEVICES POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	8/3/16	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 *2019 review waived as approval for 2018 review cycle completed end of Q1 2019	Katie Rose	Minor	Annual Review, minor wording changes and added statement re: system upgrades and patching	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

POLICY

Harris Computer Systems (Harris or Company) maintains specific protections and precautions for portable devices to reduce the potential exposure of Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information.

PROCEDURE

1. Portable Computing Devices includes but is not limited to laptops, wearables, tablets, smartphones, external drives of all types, memory cards, cds, dvds, backup media, and smart cards.
2. Only Harris approved Portable Computing Devices can be used for Company business purposes. Approval and verification of device configuration by Corporate IT is required for use of a personally owned computing device prior to connecting to the Harris network or workstations. For use of personal smartphones or tablets see Corporate Mobile Device Usage Policy and Guidelines.
3. PHI, PII and other Sensitive Information cannot be stored on Portable Computing Devices. If it is necessary to use a Portable Computing Device, it must be encrypted. Any exceptions to this requirement must be documented. The use of Portable Computing Devices to process or store PHI, PII or other Sensitive Information is restricted to only those that are managed by Harris to ensure appropriate security controls.
4. Security precautions required of Users with Portable Computing Devices include:
 - (a) Using strong passwords. For more information see the Responsible Use of IT Resources Policy and the Corporate Password Policy.
 - (b) Applying upgrades and security patches when available and appropriate.
 - (c) Using only approved applications obtained from approved application stores.
 - (d) Using only Corporate IT approved Portable Computing Devices.
 - (e) Limiting use of Portable Computing Devices to authorized users only.
 - (f) Securing unattended Portable Computing Devices.
 - (g) Avoiding the use of Portable Computing Devices, when possible.
5. Users of Portable Computing Devices are required to be knowledgeable about the device's security features.

6. Users of Portable Computing Devices are to report lost or stolen devices immediately to their supervisor, Corporate IT or the Security Officer. Failure to take appropriate action to prevent theft or to report loss of a device is a serious offense and may result in termination.
7. Users are responsible for damage and/or loss or theft of Portable Computing Devices. In order to avoid loss or theft:
 - (a) Portable Computing Devices may not be left unattended.
 - (b) Portable Computing Devices may not be checked as luggage when traveling.
 - (c) Diligence must be exercised when Portable Computing Devices are passed through airport x-ray devices such that devices will be tracked through the x-ray device and immediately collected as soon as permitted by airport security personnel.
 - (d) Portable Computing Devices will be kept out of view when left in cars; however, to the extent possible, devices shall not be left unattended in an automobile.
8. Non-company approved (visiting) devices, such as Workforce Member's, contractor's and subcontractor's personal devices must not be connected to the Company's network without permission and assistance from Corporate IT since it could be disruptive or destructive to the network. Additionally, non-company approved devices are restricted from manipulating, transporting or storing PHI, PII or other Sensitive Information.

DEFINITIONS

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

REGULATORY REFERENCES

45 C.F.R. § 164.308(a)(4)

45 C.F.R. § 164.312(a)(1)