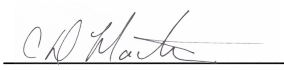
HARRIS COMPUTER SYSTEMS

CORPORATE MOBILE DEVICE POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	07/24/18	Katie Rose	Major	Standardized formatting, made revisions based on review VP of CIT and Legal.	Todd Richardson
1.1	10/22/18	Katie Rose	Minor	Annual Review in conjunction with all other policies.	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	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

Harris Computer Systems
Mobile Device Usage Policy

POLICY

Harris Computer Systems (Harris or "Company") provides greater Mobile Device choices to its workers and simultaneously reduces end-user Mobile Device complexity by providing secured company email/calendar/contacts data, mobile applications and secure intranet access on employee personal Mobile Devices. This policy describes the responsibilities, guidelines, and terms of use for employee-owned Mobile Devices configured for Harris data use.

Harris maintains specific protections and precautions for personal Mobile Devices to reduce the potential exposure of Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information.

SCOPE

1. This document applies to employees who wish to access Harris Computing Resources on a personal Mobile Device.
2. Personal Mobile Devices referenced in this document are limited specifically to those listed in this document.

ELIGIBILITY

Harris Users who are willing to agree with these policies and guidelines may use their approved personal device to access Harris Computing Resources. Harris Computing Resources include but are not limited to Corporate email, Corporate Instant Messaging applications (i.e., Teams and Skype), WorkDay, Office 365 applications and other Corporate Information Technology (CIT) supported applications made available by the CIT Mobile Device Management solution. Instructions on how to access these applications are located in this Knowledge Base Article.

APPROVED AND CERTIFIED MOBILE DEVICES FOR BYOD

Personal Mobile Devices referenced in this document are limited specifically the following:

- Android Phones and Tablets
- iPhones and iPads
- Windows Phones

RESPONSIBILITIES

1. Information Technology Responsibilities
    a. CIT is responsible for supporting the configuration of the User's Mobile Device to access Harris Computing Resources.
    b. CIT is responsible for Mobile Device access removal and performing a "remote wipe" of company data from a User's lost or stolen Mobile Device. In some situations, CIT may perform a full device wipe after providing sufficient notice to the User to allow for personal data backup.

c. CIT is responsible for Mobile Device removal and performing a "remote wipe" of Company data from a User's Mobile Device upon termination of employment with Harris.
d. Android, Windows and Apple Mobile Device Users must have Mobile Device Management software installed by CIT to continue to access Harris Computing Resources.
e. Management of the Mobile Device Management software to enforce detective and preventative controls.

2. User Responsibilities
    a. The User is responsible for using Harris Computing Resources on his or her personal Mobile Device within the same constraints as on a company-owned device by adhering to the Corporate Portable Computing Devices Policy, Corporate Responsible Use of IT Resources Policy, the Corporate Remote Access Policy and the policies and procedures referenced herein.
    b. The User will not download or transfer sensitive business data to their Mobile Device outside of managed and approved mobile Computing Resources and applications.
    c. The User will password-protect the Mobile Device and implement an automatic lockout screen.
    d. The User must maintain the original Mobile Device operating system and keep the device current with security patches and updates, as released by the manufacturer.
    e. The User agrees not to share the Mobile Device with other individuals or family members.
    f. The User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments.
    g. The User will not backup/download/transfer sensitive business data/documents to any third-party service.
    h. The User is responsible for backing up personal data and applications.
    i. The User is responsible for contacting the CIT Service Desk immediately in the event that his or her Mobile Device is lost or stolen.
    j. The User is responsible for contacting the CIT Service Desk prior to replacing their Mobile Device when possible, if not prior to, then immediately after they have replaced their Mobile Device.
    k. The User is responsible for all Mobile Device support requirements, including the cost of repairs or replacement. The company is responsible, however, for configuring and supporting the Mobile Device to receive and access Harris Computing Resources.

3. User Responsibilities (When Approved for Stipend)
    a. The User is responsible for maintaining and paying the monthly/annual fee to the telephone mobile carrier. All mobile telephone charges that he or she incurs are his or her responsibility, whether such charges are work related or for

personal use. This includes, but is not limited to, charges resulting from texts, data plan surcharges, calls, navigation, or application uses or from early termination fees.

b. The User receiving a monthly stipend is responsible for notifying the Company immediately if he or she discontinues mobile telephone service so that the stipend can be discontinued.

EXPECTATION OF PRIVACY

Harris Corporate IT will manage the configuration of the Mobile Device and, as such, will have access to information on the device including location, installed applications, data usage and other device related information.

PROCEDURE:

1. Mobile Device Setup

   Users wishing to use an approved personal mobile device to access Harris Computing Resources must complete and submit a request to the CIT Service Desk and agree by acknowledging this policy upon enrollment of the Device Management solution.
2. Mobile Device Limitation
   a. Harris allows two (2) personal Mobile Devices for Harris Computing Resources access for each participating User. Additional licenses will be based on business need and will require EVP approval.
3. Mobile Device Restrictions and Controls
   a. The Company may place various security controls and restrictions on your device such as the enforcement of a passcode and idle time lockout period.
4. Accessing Company Computing Resources
   a. As a prerequisite for accessing Harris Computing Resources on a User's personal Mobile Device, the User must first enroll their device in the Company Device Management system.
   b. Once a participating employee enrolls their approved Mobile Device and the device is configured by the Device Management system, all corporate access and data will be managed and controlled by the Device Management system.
5. Jailbroken or Rooted Devices
   a. Jailbroken Apple iOS devices and rooted Android devices pose a risk to Harris data contained within the secure communications application. Therefore, the Company will disable or remove Company data access on devices determined to be jailbroken or rooted.

USER ACKNOWLEDGMENT AND AGREEMENT

It is Harris' right to restrict computing privileges or take other administrative or legal action due to failure to comply with the above referenced Policy and Procedures. Violation of these rules may be grounds for disciplinary action up to and including termination. By enrolling in the Corporate Device Management system users acknowledge, understand and will comply with the above referenced security Policy and Procedures, as applicable to the

user's personal Mobile Devices usage of Harris Computing Resources and services. Users understand that Harris is not responsible for any loss or theft of, damage to, or failure in the personal Mobile Device that may result from use of third-party software and/or use of the device used to access Harris Computing Resources. Users understand that business use may result in increases to personal monthly service plan costs.

Should a User decide to discontinue use of a personal Mobile Device to access Harris Computing Resources or cease to become an employee of Harris or replace a personal Mobile Device, the User agrees that Harris will remove and disable any Company provided third-party software, services and Harris data from the personal device.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

42 C.F.R. § 164.312(a)

74 Fed. Reg. 19006, 19008-10 (April 27, 2009)