HARRIS COMPUTER SYSTEMS

CORPORATE WORKSTATION USE AND SECURITY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: ______________________________

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/16/2016	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, Added requirement to comply with the Remote Access Policy.	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

POLICY

The purpose of this policy is to prevent unauthorized access to information systems containing Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information. Access to information systems containing PHI, PII or other Sensitive Information is provided only to properly authorized users. Leadership approves the use of information assets to support business functions. In the event of unauthorized activity, disciplinary actions may be taken.

PROCEDURE

1. Harris Computer Systems (Harris or Company) owned computers are to be used for authorized purposes to support the business functions of the Company. Incidental personal use is permitted only in accordance with the Harris Employee Handbook and the Responsible Use of IT Resources Policy.

2. Harris maintains an inventory of the types and locations of Company owned computers, which is updated as assets, are acquired, transferred, moved or removed (i.e., destroyed, purged, lost or stolen). See Asset Tracking Policy.

3. Any personally owned computer used for Harris business, local or remotely, must be reviewed and approved by Corporate IT prior to connecting to Harris networks. See the Responsible Use of IT Resources Policy and the Personal Mobile Device Usage Policy for more information.

4. Harris owned computers containing or with access to PHI, PII or other Sensitive Information are located in physically secure areas and their display screens are positioned such that information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception, public, or other related areas so as to prevent unauthorized viewing of PHI, PII or other Sensitive Information. Workforce Members authorized to work remotely must also comply with the Remote Access Policy.

5. Users shall not use Harris owned computers to engage in any activity that is either illegal under local, state, federal, provincial or international law or is in violation of Company policy.

6. Users must adhere to the Company's Responsible Use of IT Resources Policy, Asset Tracking Policy, Backup, Device and Media Controls Policy and Email Policy.

7. Access to all Harris owned computers containing PHI, PII or other Sensitive Information is controlled by reasonable and appropriate authentication methods. Unique users IDs and passwords are used and activity for unique users IDs and passwords is tracked.

8. When an Workforce Member, contractor, subcontractor or other user of Harris owned computers leaves the Company, their information system privileges, both internal and remote, are disabled or removed by the time of departure. Special attention is paid to situations where a privileged access user terminates, or a user terminates who poses a risk to information or systems.

9. Workforce Members must at a minimum lock their computers when not occupying it. Workforce Members must shutdown or at a minimum log off from or lock their computer(s) when their shifts are complete. A user identification and password is required to gain re-entry. See the Security Awareness and Training Policy.

DEFINITIONS

See attached policy definitions or click

here.

REGULATORY REFERENCES

45 C.F.R. § 164.308(a)(5)
45 C.F.R. § 164.310(b) and (c)