HARRIS COMPUTER SYSTEMS

CORPORATE ACCESS CONTROL POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: ______________________________

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/10/16	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, Clarified role based access, added statement re: use of generic accounts, requirement for separate administrative accounts, changed inactivity time from 30 to 15 minutes	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

To implement technical policies and procedures for electronic systems or software programs that maintain Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information to allow access only to those persons or software programs that have been authorized to access PHI, PII or other Sensitive Information and to be compliant as a Business Associate of Covered Entities where appropriate.

POLICY

Access to Harris Computer Systems (Harris or Company) applications or systems with PHI, PII or other Sensitive Information is only provided to Workforce Members based on their specific job requirements and is determined on a case-by-case basis. All Workforce Members do not have access to the same systems or software programs. Access to privileged functions, security and relevant information is restricted as appropriate. An example for illustrative purposes, but not meant to be an exhaustive explanation, would be an administrative assistant, who has no need to access PHI, PII or other Sensitive Information and would therefore not be granted access to the systems or applications containing PHI, PII or other Sensitive Information. Users must use encryption when sending, receiving or storing PHI, PII or other Sensitive Information on all media types. Furthermore, such access is routinely examined and validated based on need.

The full path to instructions on how to send encrypted email is:

https://harriscomputer.lightning.force.com/lightning/r/a3Q1500000017OaEAI/view

SCOPE

1. This policy applies to Harris employees, management, contractors, student interns, and volunteers (herein referred to collectively as the Workforce).
2. This policy describes Harris' objectives and policies regarding maintaining the security of PHI, PII or other Sensitive Information.

PROCEDURE

1. Unique User/Identification.

   a. All Workforce Members with access to Harris' network(s) containing PHI, PII or other Sensitive Information are assigned a unique user identification to log in to network system or application. Users maintain their own passwords. Any software that uses PHI, PII or other Sensitive Information also requires a company assigned identification and user owned password (separate from the operating system identification and password). All passwords must be maintained in accordance with the Corporate Password Policy.

b. Workforce Members are strictly prohibited from sharing user identifications and passwords. Violations of this prohibition can result in sanctions up to and including termination.

c. Workforce Members are granted access to information and systems based on their role or function.

d. Shared or generic User ID's may not be used unless there is legitimate business need that has been pre-approved by the information or system owner. An owner must be identified for any shared or generic User ID and the terms of the Corporate Password Policy must be applied to the User ID.

e. Separate User ID's must be used for administrative or privilege access and are authorized by the system owner. The Corporate Password Policy must be applied to administrative or privilege User ID's.

f. User account types are identified (i.e., shared, system, application, individual, etc.) to determine group memberships and changes are made to the groups as appropriate when user roles change or when a user is terminated.

g. The Security Officer in conjunction with the Information or System Owner will routinely audit to ensure that user rights remain appropriate given the job description of each Workforce Member. The Security Officer will assist with the audit as required.

h. Any authorized user must at a minimum lock their workstation when not occupying it. A user identification and password are required to gain re-entry.

2. Emergency Access Procedure. If any Harris internal system and application requires immediate access, the Security Officer and IT support will work together to determine the nature of the emergency and the steps necessary to provide services in the emergency.

a. The determination of who will have emergency access, if any, will be made by the Security Officer at the time of the emergency. If the Security Officer is unavailable, the Privacy Officer will make the determination.

3. Automatic Logoff. Sessions to systems or applications will automatically timeout after no more than 15 minutes of inactivity. End users are required to provide a password to log into systems or applications after 15 minutes of inactivity. Further,

all users must activate their workstation locking software whenever they leave their workstation unattended for any length of time.

4. Encryption and Decryption. All senders and receivers of email with potential PHI, PII or other Sensitive Information must use encryption. Instructions on how to encrypt email are detailed above.

   a. All other PHI, PII or other Sensitive Information maintained by Harris must be encrypted by the Information Owner responsible for managing the data. If encryption of PHI, PII or other Sensitive Information is not possible, appropriate counter measures to protect this information must be established.

   b. Valid encryption processes include those identified by the following standards, processes that are Federal Information Processing Standards (FIPS), or others that may be identified from time to time by the Secretary.

      For data at rest:
      CCS CSC 17; COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.0; ISA 62443-3-3:2013 SR 3.4, SR 4.1; ISO/IEC 27001:2013 A.8.2.3; NIST SP 800-53 Rev. 4 SC-28

      For data in transit:
      CCS CSC 17; COBIT 5 APO01.06, DSS06.06; ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2; ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3; NIST SP 800-53 Rev. 4 SC-8

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)