HARRIS COMPUTER SYSTEMS

CORPORATE SECURITY MANAGEMENT

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/18/16	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	Major	Annual Review, Introduced the GRCC, added Security Officer qualifications requirements, removed Risk Analysis components.	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document, Added data integrity statement, changed ePHI to PHI where it made sense	Dwayne Martin

POLICY

Harris Computer Systems (Harris or "Company") maintains a reasonable process to review its security management systems in order to identify any risks to Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information and the adoption of reasonable and appropriate measures to reduce any risks and vulnerabilities. Harris leadership assigns a qualified Information Security Officer who obtains industry recognized security certifications and appropriate years of experience. The Security Officer is responsible for information security and is part of the Governance, Risk and Compliance Committee (GRCC) that governs the Information Security Management Program and this policy. Harris leadership supports the GRCC and appoints members by name as appropriate. Members of the GRCC includes but is not limited to Senior Legal Counsel, the Corporate Privacy Officer, the Director of Compliance and the Security Officer. Security contacts are appointed for each business unit as appropriate.

The Company on a regular basis, monitors compliance with its Information Security Policies, Procedures and Standards and reviews and updates its Information Security Management Program. In addition, the Company will ensure that its approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) by the GRCC and key stakeholders is appropriate. Key performance indicators and other metrics are used as appropriate to determine compliance, findings are documented and maintained to monitor the Company's security posture. The Company will also follow procedures to assess risk and impact to the security and integrity of PHI, PII or other Sensitive Information when implementing changes to its information systems.

This policy applies to all systems and all PHI, PII or other Sensitive Information maintained, used or disclosed by the Company including the creation, receipt, maintenance and transmission of PHI, PII or other Sensitive Information.

PROCEDURE

1. Risk Management
    a. The Security Officer is responsible for the security management process and ensuring that systems that contain, process or transmit PHI, PII or other Sensitive Information have been identified and documented. The security management process includes the assessment of the administrative, physical and technical aspects of the security management of the Company. (See the Security Management Tool in the Risk Assessment and Analysis Policy.)
    b. The Security Officer is responsible for ensuring the Company's Information Security Management Program is reviewed annually to assess the effectiveness of the program and its associated controls, compliance with the policies, procedures and standards, or when significant changes to the security implementation occur. If an external

consultant is used to conduct the review, an agreement must be in place with the consultant that includes verification of the consultant's credentials and experience.

c. The review will include all elements of industry standards, the Security Rule when appropriate and security best practices necessary to conduct the evaluation.
d. The results of the review will be documented and reported to management. The Security Officer is responsible for ensuring that, where applicable, appropriate corrective or remedial action is taken.
e. As a part of the security management process, the Security Officer will implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports as required by existing policies and procedures attached herein. Security testing, training and monitoring of activities will also be conducted as appropriate for the risk management of systems and data.

2. Vulnerability Management
    a. The Information or System Owner is responsible for ensuring vulnerability assessments are conducted per Business Associate Agreements and regulatory compliance requirements with assistance from the Information Security Officer.
    b. Vulnerability assessments will include technical vulnerability testing and assessing risks of identified vulnerabilities as it relates to the system and/or data criticality according to industry standards and security best practices necessary.
    c. The results of the assessment will be documented and reported to management as appropriate.
    d. The Security Officer is responsible for ensuring that, where applicable, appropriate corrective or remedial action is taken.
    e. Penetration testing may be conducted on systems or applications as appropriate which will be determined by key stakeholders. A thorough risk assessment will be conducted before engaging in penetration testing to determine the likelihood and impact in the event of an adverse effect of such testing.

3. Change Management
    a. The Security Officer will participate in the change management process (*See* Corporate Change Control Policy) to ensure the appropriate security controls and safeguards are considered during the change process.
    b. When appropriate, the Security Officer will review and provide approval of new software, hardware or service before it is installed or connected to the Company's networks.

c. Before approving a change request, the Security Officer will conduct a risk analysis to assess the vulnerabilities, impact and risks related to PHI, PII or other Sensitive Information that are associated with the proposed change.

4. Data Security

a. The Company implements technical controls to ensure PHI, PII or other Sensitive Information is stored as specified by the Company. PHI, PII or other Sensitive Information at rest is protected using an encryption method appropriate to the medium where it is stored. If the Company does not encrypt PHI, PII or other Sensitive Information, a documented rationale for not doing so is maintained or alternative compensating controls are used, and the method is approved by the Security Officer or key stakeholders and reviewed annually.

b. The Company restricts the location of facilities that process, transmit or store PHI, PII or other Sensitive Information (e.g., to those located in the United States), as needed, based on its legal, regulatory, contractual and other security and privacy-related obligations.

c. The Company implements technical, physical and administrative controls to ensure the integrity of PHI, PII or other Sensitive Information as appropriate. Access to PHI, PII or other Sensitive Information is granted to Workforce Members who require the information to accomplish the work responsibilities of their position and is granted on a minimum necessary or need-to-know basis. Hardware, software, and procedural auditing mechanisms are implemented on the information systems used that contain or use PHI, PII or other Sensitive Information and audit logs are reviewed regularly.

5. Documentation

The Security Officer is responsible for documenting and maintaining the information security management procedures and information security management reviews and approvals.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

45 C.F.R. § 164.308

National Institute of Standards and Technology Special Publication 800-30 REV 1, *Risk Management Guide for Information Technology Systems*.