HARRIS COMPUTER SYSTEMS

CORPORATE SECURITY RISK ASSESSMENT AND ANALYSIS

Corporate Officer: Dwayne Martin, Vice President

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	Initial version of policy. The Risk Analysis section was originally in the Security Management Policy and moved to this policy. Incorporated the Risk Assessment process.	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, added review of risk analysis, included Change Management process in risk analysis process and changed PHI to PHI; Inserted Definitions Document	Dwayne Martin

Harris Computer Systems
Corporate Risk Assessment and Analysis Policy

POLICY

Harris Computer Systems (Harris or Company) continues 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. 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 ensures that its approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) is reviewed at planned intervals or when significant changes to the security implementation occur. The Company also follows 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.

The Security Officer in conjunction with the Governance, Risk and Compliance Committee (GRCC), key management staff and the IT Department will conduct security risk assessments as needed and risk analyses on an annual basis or in response to environmental and operational changes. A vulnerability assessment may also be conducted periodically as required. The Security Officer in conjunction with the GRCC will determine if an analysis should be conducted by internal staff or whether an outside consultant should be engaged. If an outside consultant is engaged, a written agreement must be in place with the consultant which includes a verification of the consultant's credentials and experience. An outside consultant will be engaged at least once every three years.

This policy applies to all systems and all PHI, PII or other Sensitive Information maintained, used or disclosed by the Company and will include the creation, receipt, maintenance and transmission. Any revisions to policies and procedures in conducting assessments will be administered by the Security Officer in conjunction with the GRCC and documented.

PROCEDURE

1. Risk Assessment
    a. The Security Officer in conjunction with the GRCC and key management will assess risks of security incidents and vulnerabilities to determine the potential impact to the Company systems and information.
    b. The risk assessment will include the impact to systems or PHI, PII or other Sensitive Information, the level of response required for remediation or mitigation of the risk and notification requirements.
    c. The Security Officer in conjunction with the GRCC and key management will ensure appropriate actions are taken in response to vulnerabilities or security incidents being assessed.

d. The Security Officer in conjunction with the GRCC and key management will ensure the security incident is documented according to the Corporate Incident Response Procedures.
e. Once the risk assessment has been completed, the Security Officer in conjunction with the GRCC is responsible for the development and updating of policies and procedures to implement any reasonable and appropriate measures to mitigate any vulnerabilities or risk of further security incidents.

2. Risk Analysis

a. The Security Officer in conjunction with the GRCC is responsible for conducting a risk analysis to assess the potential risks and vulnerabilities of PHI, PII or other Sensitive Information.
b. The risk analysis will identify all information systems with access to or that maintain PHI, PII or Sensitive Information. The risk analysis will also identify those information systems and associated data that are critical to the Company continuing business operations.
c. The risk analysis will consider all relevant losses that would be expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. The degree of response is determined by the risks identified and is reviewed during the Change Management process and during the annual policy review.
d. All elements of the Security Rule should be considered when conducting risk analysis. The Security Management Tool should be used as a guide for risk analysis.
e. All necessary information to conduct the analysis will be obtained by internal staff or the outside consultant conducting the analysis.
f. All analysis findings, remediation options, acceptances, recommendations and remediation decisions will be documented and maintained by the Security Officer in conjunction with the GRCC in the Governance Risk and Compliance (GRC) tool for no less than three years.
g. Once the risk analysis has been completed, the Security Officer in conjunction with the GRCC is responsible for the development and updating of policies and procedures to implement any reasonable and appropriate measures to mitigate any risks or vulnerabilities identified. Risk assessments are re-evaluated at least annually or when significant changes occur in the environment to ensure risks are addressed where appropriate.
h. As part of the Risk Analysis an eight-step risk assessment process is followed which includes:

i. *PHI boundary definition*. A boundary definition includes an inventory of information system hardware and software details, including (i) internal and external interfaces, (ii) the identification of primary users of the information systems of PHI, PII or other Sensitive Information (iii) basic function and purpose of the PHI, PII or other Sensitive Information and information system, and (iv) technical controls (i.e., encryption) and non-technical controls (i.e., policies and procedures.)

ii. *Threat identification*. Potential and actual threats to PHI, PII or other Sensitive Information will be identified and logged. The confidentiality of PHI, PII or other Sensitive Information will be determined by analyzing the risk of improper access to stored information, and by the risk of interception during electronic transmission of the information.

iii. *Vulnerability identification*. Vulnerability identification will be accomplished and logged by identifying how and why the PHI, PII or other Sensitive Information has been threatened.

iv. *Security control analysis*. A security control analysis will be conducted and logged by reviewing, for example, logs, access reports, and incident tracking. A determination will be made from that review as to whether the controls are adequately preventing threats.

v. *Risk likelihood determination*. A determination of the likelihood of risk will be conducted by reviewing the security control analysis and comparing it to potential and actual threats and vulnerability. This data will be logged.

vi. *Impact analysis*. An impact analysis will be conducted by determining whether new or modified security safeguards and procedures beyond what the Company has in place should be established. This data will be logged.

vii. *Risk determination*. The Company will determine what PHI, PII or other Sensitive Information is at risk and will record such information.

viii. *Security control recommendations*. Utilizing all of the information gathered in the risk analysis, The Company will develop security control recommendations and will record such information. The Security Officer, and when appropriate, in conjunction with the

Privacy Officer, will make the determinations as to the controls to utilize.

b. The risk analysis will consider all relevant losses that would be expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. The degree of response is determined by the risks identified.

c. In addition to the annual risk analysis, the Security Officer will conduct appropriate risk assessment when an environmental or operational change would impact the flow of PHI, PII or other Sensitive Information.

d. Once the risk analysis has been completed, the Security Officer is responsible for the development and updating of policies and procedures to implement any reasonable and appropriate measures to mitigate any risks or vulnerabilities identified.

Security Management Tool

(R) means "**required**." The term "required" means the implementation of the specification is mandatory.

(A) means "**addressable**." The term "addressable" means that the Company must assess whether the implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed in relation to the likely contribution of the specification to protecting PHI accessed, maintained or transmitted by the Company. An addressable specification is not optional.

If the specification is determined to be reasonable and appropriate, it must be implemented.

If the specification is determined not to be reasonable and appropriate, the Company must: document why it would not be reasonable and appropriate to implement the specification; and implement an equivalent alternative measure if reasonable and appropriate.

Standards	**Implementation Specifications**	**Rule**	**Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)**
Administrative Safeguards			
Security Management Process Section 164.308(a)(1) General Rule: Implement policies and procedures to prevent, detect, contain, and correct security violations.	**Risk Analysis** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI.	(R)	
	Risk Management Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level	(R)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
	Sanction Policy Apply appropriate sanctions against Workforce Members who fail to comply with the security policies and procedures.	(R)	
	Information System Activity Review Implement procedures to regularly review records of Information System activity, such as audit logs, access reports, and Security Incident tracking reports.	(R)	
Assign Security Responsibility Section 164.308(a)(2)	Appoint a Security Officer who is responsible for the development and implementation of the policies and procedures for electronic security.	(R)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Workforce Security Section 164.308(a)(3) General Rule: Implement policies and procedures to ensure that all employees have access to PHI as appropriate for their duties, and to prevent those employees who do not have access from obtaining access to PHI.	**Authorization and/or Supervision** Implement procedures for the authorization and/or supervision of employees who work with PHI or in locations where it might be accessed.	(A)	
	Workforce Clearance Procedures Implement procedures to determine that the access of employees to PHI is appropriate.	(A)	
	Termination Procedures Implement procedures for terminating access to PHI when an employee is no longer authorized to access PHI (e.g., termination of employment, transfer to a new position, change in duties) (collectively, referred to as "Access Termination").	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Information Access Management Section 164.308(a)(4) General Rule: Implement policies and procedures for authorizing access to PHI.	**Access Authorization** Implement policies and procedures for granting access to PHI. For example, through access to a workstation, transaction, program, process, or other mechanism.	(A)	
	Access Establishment and Modification Implement policies and procedures that, based upon the Company's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	(A)	
Security Awareness and Training Section 164.308(a)(5) General Rule: Implement a security awareness and	**Security Reminders** Implement policies and procedures that provide for periodic security awareness updates. Implement a training program to train all existing employees and new employees.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
training program for all members of the workforce (including management).	**Protection from Malicious Software** Implement policies and procedures for guarding against, detecting, and reporting malicious software.	(A)	
	Log-in Monitoring Implement policies and procedures for monitoring log-in attempts and reporting discrepancies.	(A)	
	Password Management Implement policies and procedures for creating, changing, and safeguarding passwords.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Security Incident Procedures Section 164.308(a)(6) General Rule: Implement policies and procedures to address Security Incidents.	**Response and Reporting** Implement policies and procedures (1) to identify and respond to suspected or known security incidents; (2) to mitigate, to the extent practicable, harmful effects of security incidents that are known; and (3) to document security incidents and their outcomes.	(R)	
Contingency Planning Section 164.308(a)(7) General Rule: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages	**Data Backup Plan** Establish and implement policies and procedures to create and maintain retrievable exact copies of PHI.	(R)	
	Disaster Recovery Plan Establish (and implement as needed) policies and procedures to restore any loss of data.	(R)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
systems that contain PHI (e.g., fire, vandalism, system failure, and natural disaster).	**Emergency Mode Operation Plan** Establish (and implement as needed) policies and procedures to enable continuation of critical business processes for protection of the security of PHI while operating in emergency mode.	(R)	
	Testing and Revision Procedures Implement policies and procedures for periodic testing and revision of contingency plans.	(A)	
	Application and Data Criticality Analysis Assess the relative criticality of specific applications and data in support of other contingency plan components.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Evaluation Section 164.308(a)(8)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the security rule and, subsequently, in response to environmental or operational changes affecting the security of PHI, which evaluation establishes the extent to which the security policies and procedures meet the requirements of the rule.	(R)	
Business Associate Agreements and Other Contract Arrangements Section 164.308(b)(1)	Maintain written contracts that reflect Business Associate requirements	(R)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Physical Safeguards			
Facility Access Controls Section 164.310(a)(1) General Rule: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	**Contingency Operations** Establish (and implement as needed) policies and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	(A)	
	Facility Security Plan Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
	Access Control and Validation Procedures Implement policies and procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision.	(A)	
	Maintenance Records Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security. (For example, hardware, walls, doors, and locks.)	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Workstation Use Section 164.310(b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access PHI.	(R)	
Workstation Security	Implement physical safeguards for all workstations that access PHI, to restrict access to authorized users.	(R)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Device and Media Controls Section 164.310(d) General Rule: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI	**Disposal** Implement policies and procedures to address the final disposition of PHI, and/or the hardware or electronic media on which it is stored.	(R)	
	Media Re-Use Implement policies and procedures for removal of PHI electronic media before the media are made available for re-use.	(R)	
	Accountability Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	(A)	
	Data Backup and Storage Create a retrievable, exact copy of PHI, when needed, before movement of equipment.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Technical Safeguards			
Access Control Section 164.312(a)(1) General Rule: Implement technical policies and procedures for electronic information systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights.	**Unique User Identification** Assign a unique name and/or number for identifying and tracking user identity.	(R)	
	Emergency Access Procedure Establish (and implement as needed) policies and procedures for obtaining necessary PHI during an emergency.	(R)	
	Automatic Logoff Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	(A)	
	Encryption and Decryption Implement a mechanism to encrypt and decrypt PHI.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Audit Controls Section 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.	(R)	
Integrity Section 164.312(c)(1)	**Mechanism to Authenticate PHI** Implement electronic mechanisms to corroborate that PHI has not been altered or destroyed in an unauthorized manner.	(A)	
Person or Entity Authentication Section 164.312(d)	Implement policies and procedures to verify that a person or entity seeking access to PHI is the one claimed.	(R)	
Transmission Security Section 164.312(e)(1) General Rule: Implement technical security measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network.	**Integrity Controls** Implement security measures to ensure that electronically transmitted PHI is not improperly modified without detection until disposed of.	(A)	
	Encryption Implement a mechanism to encrypt PHI whenever deemed appropriate.	(A)	

Standards	Implementation Specifications	Rule	Description of Risk Analysis and Security Measures Adopted (include policies and procedures and documentation)
Organizational Requirements			
Business Associate Agreements Section 164.314(a)	Amend Business Associate agreements to add electronic security language. Implement process to ensure contracts address confidentiality, integrity and availability of PHI	(R)	
Policies and Procedures Section 164.316	Document in writing all of the policies and procedures required for PHI. Must be maintained for six years from the date of creation or the date when they were last in effect, whichever is later.	(R)	

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*.