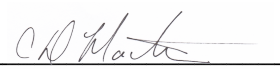
HARRIS COMPUTER SYSTEMS

CORPORATE INFORMATION ACCESS MANAGEMENT POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/22/16	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	Katie Rose	Minor	Annual Review, added the responsibility of the GRCC and HR	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

POLICY

Harris Computer Systems (Harris or Company) is committed to controlling, managing and monitoring access to Protected Health Information (PHI), Personally Identifiable Information (PII), or other Sensitive Information by requiring authorization before access to PHI, PII or other Sensitive Information is granted.

Access to PHI, PII or other Sensitive Information is only 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. Business Associate Agreements, non-disclosure agreements or other agreements as appropriate will be in place prior to non-Harris use or system access being granted to information or systems that contain PHI, PII or other Sensitive Information. Access is specified, documented and reviewed annually.

PROCEDURE

1. Access Authorization

    a. The Governance Risk and Compliance Committee (GRCC) in conjunction with Human Resources define processes by which access information systems containing PHI, PII or other Sensitive Information is authorized. Access is generally granted based on role to ensure segregation of access to only the access required to perform assigned duties.

    b. PHI, PII or other Sensitive Information and systems containing PHI, PII or other Sensitive Information can only be accessed by those who have been authorized by the appropriate Information Owner and assigned access rights.

    c. Harris Workforce Members, contractors and subcontractors are not allowed access and may not attempt to gain access to Harris information systems, including, but not limited to those containing PHI, PII or other Sensitive Information, until or unless they are given proper authorization.

    d. Requests for access are submitted using a ticketing system that logs the request and approval.

    e. Access authorization for new Workforce Members will be performed in compliance with the Employee Onboarding Procedure below.

    f. All Workforce Members with access to Company information systems will be assigned a unique user identification. See the Corporate Password Policy and the Corporate Responsible Use of IT Resources Policy.

2. Access Establishment and Modification

   a. The GRCC ensures that access rights to Company information systems containing PHI, PII or other Sensitive Information is periodically reviewed by the Information Owner to ensure that they are provided only to those who have a need for specific PHI, PII or other Sensitive Information in order to accomplish a legitimate task.

   b. Occasionally, required access to PHI, PII or other Sensitive Information may change. The GRCC ensures that any modifications are reviewed by the Information Owner in a timely manner and act accordingly. If the modification is the result of a termination, then the access will be terminated immediately and in accordance with the Employee Termination Policy below.

   c. All revisions to Harris Users access rights are tracked, logged and audited.

3. Employee On-Boarding Procedure

   a. As part of the personnel hiring process, the hiring manager, Human Resources, with the Privacy Officer, will ensure that new employees have the necessary knowledge, skills, and abilities to fulfill roles involving access to and use of Sensitive Information.

   b. All new and transferred Workforce Members, contractors and subcontractors whose roles and responsibilities may expose them to PHI, PII or other Sensitive Information will receive HIPAA and Information Security Training as soon as possible, preferably prior to accessing any PHI, PII or other Sensitive Information but not later than 90 days after employment or transfer.

   c. All hardware provided to a new employee is documented before the equipment is given to the employee. See the Corporate Asset Tracking Policy for more information.

4. Employee Termination Procedure

   a. A departing Workforce Member's manager will immediately notify Human Resources of the resignation or termination and the last day of employment via the Human Resources management tool. Human Resources will immediately notify CIT of a Workforce Member's resignation or termination and the last day of employment by automated ticketing processes where applicable. The same shall apply to any non-employee Workforce Member who has been provided with credentials to access PHI, PII or other Sensitive Information.

b. The departing employee's login credentials and information access permissions will be deactivated prior to or simultaneous with the Workforce Member's, contractor's or subcontractor's departure.

c. All Harris equipment and hardware must be returned prior to the Workforce Member's and where applicable the contractor's or subcontractor's departure from the Company. If property is not returned, it will be pursued. For the protection of PHI, PII or other Sensitive Information, failure to return property will result in further legal action. Serial numbers on the equipment returned will be verified to match the serial numbers recorded at the time the equipment was issued to the Workforce Member, contractor or subcontractor

d. Harris will have an exit interview, whenever possible, with departing Workforce Members, contractors or subcontractors as part of the exit interview to remind them of their obligations to maintain confidentiality of any PHI, PII or other Sensitive Information.

e. Access rights will be reviewed to ensure that departing Workforce Member's, contractor's or subcontractor's access rights were effectively and entirely terminated prior to or simultaneously with their departure.

ROLES AND RESPONSIBILITIES

1. The Vice President of Corporate Information Technology (VP of CIT) or equivalent has the following security policy and planning responsibilities:

   - Designating an Information Security Officer who will carry out the responsibilities of the VP of CIT for security planning;
   - Developing, maintaining and enforcing information security policies, procedures, and control techniques to address system security planning;
   - Managing the identification, implementation, and assessment of common security controls;
   - Ensuring that personnel with significant responsibilities for security policies and plans are trained;
   - Assisting Company leadership with their responsibilities for security policies and plans; and
   - Identifying and developing common security controls for the Company.

2. The Privacy Officer works to maintain a balance between security and privacy requirements and works to ensure that one is not compromised for the sake of the other. The Privacy Officer has the following responsibilities related to security policies and plans:

   - Developing, promoting, and supporting the Company's privacy program;

- Encouraging awareness of potential privacy issues and policies; and
- Reviewing and implementing privacy regulations and legislation.
- Work in conjunction with the GRCC to ensure the security and privacy of Company systems and data.

3. The Security Officer has the following responsibilities related to security policies and plans:

    - Carrying out the VP of CIT's responsibilities for security policies and planning;
    - Coordinating the development, review, and acceptance of security policies and plans with Information System Owners, Information Owners and the executive management of the Company;
    - Coordinating the identification, implementation, and assessment of the common security controls; and
    - Possessing professional qualifications, including training and experience, required to develop and review security policies and plans.
    - Work in conjunction with the GRCC to ensure the security and privacy of Company systems and data.

4. Governance, Risk and Compliance Committee - Members of the GRCC includes but is not limited to Senior Legal Counsel, the Corporate Privacy Officer, the Director of Compliance and the Information Security Officer.
    - Work GRCC to ensure the security and privacy of Company systems and data.
    - Follow procedures to assess risk and impact to the security and integrity of PHI, PII or other Sensitive Information.
    - Review security policies and processes by following the Plan, Do, Check, Act (PDCA) process.

5. Compliance Officer - The Compliance Officer works to ensure the Company has a clearly defined program for compliance of global laws and regulations. The Compliance Officer has the following responsibilities related to security policies and plans:
    - Developing, promoting, and supporting the Company's compliance program;
    - Encouraging awareness of global laws and regulations;
    - Assist in reviewing and implementing Company policies to ensure Company compliance to global laws and regulations.
    - Work in conjunction with the GRCC as required to ensure Company compliance of global laws and regulations.

6. The Information Owner has the following responsibilities related to security policies and plans:

- Providing input to Information System Owners on the security requirements and security controls for the information systems where the information resides;
- Deciding who has access to the information system and determining what types of privileges or access rights;
- Reviewing any modifications to access rights and ensuring it is appropriate; and
- Assisting in identifying and accessing the common security controls where the information resides.

7. The Information System Owner has the following responsibilities related to security policies and plans:

    - Developing the system security plan in coordination with Information Owners, the system administrator, the Security Officer and users;
    - Maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements; and
    - Ensuring that system Users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) and assisting in the identification, implementation, and assessment of the common security controls.

8. Users have the responsibility for knowing and understanding the confidentiality of the information they are using to accomplish their assigned work and ensure proper handling of information.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

45 C.F.R. § 164.308(a)(3)
45 C.F.R. § 164.308(a)(4)