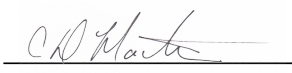
HARRIS COMPUTER SYSTEMS

CORPORATE SECURITY AWARENESS AND TRAINING PROGRAM POLICY

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	Renamed titled this document to a "Program", added content around Compliance Training, Training Content and Phishing Campaigns	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

Harris Computer Systems
Corporate Security Awareness and Training Policy

POLICY

Harris Computer Systems (Harris or Company) maintains a security awareness and training program for all Workforce Members to ensure an understanding of the roles and responsibilities of Workforce Members with access to Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information as well as the Information Security Policies, Procedures and Standards. This policy is reviewed annually for its effectiveness or when significant changes occur that impact the need for changes to security awareness and training procedures.

PROCEDURE

1. Security Reminders. , The Security Officer reminds Workforce Members of security issues and protocols periodically and as needed

   Security & Privacy Training. The Security Officer in conjunction with the Privacy Officer will ensure a formal security awareness and training program, including relevant compliance training requirements (Security Training Program), is developed and implemented. The Security Officer in conjunction with the Governance, Risk and Compliance Committee (GRCC) will review and approve the Security Training Program. The Security Officer in conjunction with Human Resources (HR) and the GRCC will ensure that the Security Awareness and Training Program is uniformly delivered to all new Workforce Members, contractors and vendors where appropriate, within 90 days of employment or transfer and annually thereafter. All Workforce Members who work with PHI must complete the required HIPAA training prior to being granted system or network access to PHI, PII or other Sensitive Information.
   The Security Officer in conjunction with HR and the GRCC will ensure that security and privacy training is accurately delivered to all Workforce Members, contractors and vendors where appropriate. Security and privacy training will be tracked and documented to include the Workforce Members trained, the date of training and a brief summary of the training subject matter or a copy of the training material.

2. Compliance Training - All Workforce Members, contractorsor vendors where appropriate, who work with PHI must complete the required HIPAA training prior to being granted system or network access to PHI, PII or other Sensitive Information. Employees from acquisition that have a documented record of training within the last 12 months are not required to attend HIPAA training within 90 days of onboarding. Documentation should include the content of the training as well as when it was administered, to whom, and how frequently. An example of acceptable documentation would be a report from a learning management system together with a course description.

All Workforce Members, contractorsor vendors where appropriate who work with data that is governed by the European General Data Protection Regulation (EU GDPR) must complete the required EU GDPR training prior to being granted system or network access PHI, PII or other Sensitive Information. Employees from acquisition have documented record of training within the last 12 months are not required to attend EU GDPR training within 90 days of onboarding.

Specific state privacy law compliance training will be delivered on an annual basis or as required to Workforce Members, contractorsor vendors where appropriate.

The Director of Compliance in conjunction with HR and the GRCC will ensure that compliance training is accurately delivered to all Workforce Members, contractorsand vendors where appropriate. Compliance training is tracked and documented to include the date of training and a brief summary of the training subject matter or a copy of the training material.

3. Record Retention - Training records are maintained for a minimum of six years. Hiring managers may contact HR to coordinate expedited training for new or transferred employees who will be working with PHI.

4. Training Content – Content of security awareness and data protection training will be appropriate to the roles of the Workforce Members, contractorsand vendors. Training content will include but is not limited to safeguards and processes for the protection of PHI, PII, phishing campaigns, identifying insider threats, incident response and other areas as needed.

5. Training Plan – The GRCC in conjunction with HR and the GRCC will determine the training course requirements for Workforce Members, contractors or vendors where appropriate, based on roles, titles and responsibilities. The Security Officer in conjunction with HR and the GRCC will ensure that the training plan is accurately delivered to all Workforce Members, contractors and vendors where appropriate. The training plan is documented to include processes for assigning security, privacy and compliance training.

6. Phishing campaigns are conducted as needed and appropriate to make users aware of the security risks of clicking links and responding to unsolicited emails or emails from senders who were not verified.

7. Review - Security Policies and Procedures will be reviewed and updated with any new technology, applicable regulations and practices on an annual basis. Training materials will be updated to reflect any new or amended Security Policies and Procedures as necessary. The Security Officer in conjunction with HR will ensure that appropriate Workforce is aware of and trained on any new or amended Security Policies, Procedures or Standards.

8. Protection of Malicious Software - Harris' Workforce will be informed of the importance of protecting against malicious software and exploitation of vulnerabilities and the procedures for guarding against, detecting and reporting malicious software as outlined in the Protection from Malicious Software Policy.

9. Log-in Monitoring - Harris' Workforce will be informed of Corporate IT procedures for monitoring log-in attempts, reporting discrepancies to the Security Officer and following the procedures for reviewing, investigating and taking corrective action with regard to potential security exposures as outlined in the Audit Controls Policy and Data Incident Policy.

10. Password Management – Workforce Members will be informed of the Company's procedures for creating, changing, and safeguarding passwords. Workforce Members must follow the minimum password requirements as outlined in the Corporate Password Policy. The Security Officer will annually review password settings for any discrepancies and to ensure compliance with the policy. Appropriate action is taken to ensure conformance to the policy and to update the policy as necessary. Any deviations from the baseline standards are documented along with the business justification for the deviation.

11. Data Incidents - Workforce Members will be informed of the Company's procedures for addressing data incidents per the Data Incident Policy and the Incident Response Procedures.

DEFINITIONS

See attached policy definitions or click

here. **REGULATORY REFERENCES**

45 C.F.R. 164.308(a)(5)