HARRIS COMPUTER SYSTEMS

CORPORATE INFORMATION SECURITY MANAGEMENT PROGRAM POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	1/15/2018	Katie Rose	Major	Initial Document	Dwayne Martin
1.1	12/4/2019	Katie Rose	Minor	Annual Review	Dwayne Martin
1.2	3/25/2020	Katie Rose	Minor	Annual Review	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review	Dwayne Martin

Harris Computer Systems
Corporate Information Security Management
Program Policy

POLICY

Harris Computer Systems (Harris) maintains an Information Security Management Program to ensure the confidentiality, integrity and availability of its systems and information. 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 on a regular basis, monitors compliance with its Information Security Policies, Procedures and Standards and reviews and updates its Information Security Management Program. This ISMP Policy is written to align with industry standard security frameworks and best practices such as the National Institute of Standards and Technology (NIST) and the information security management standards of the International Organization of Standardization (ISO 27001). Leadership allocates resources as needed and appropriate to support this ISMP. This and all associated security policies are located on the Corporate Information Technology (CIT) SharePoint site.

In addition, Harris will ensure that it's 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. Harris 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 that are used by Harris or its employees to maintain, use or disclose PHI, PII or other Sensitive Information and will include the creation, receipt, maintenance, and transmission of PHI, PII or other Sensitive Information.

As part of the Information Security Management Program, Harris Corporate Information Security Policies are in effect to ensure the confidentiality, integrity and availability of systems and information. Workforce Members are responsible for reviewing and adhering to these policies and are required to acknowledge this ISMP Policy annually. Any violation by a Workforce Member of the ISMP or associated policies and procedures will be grounds for disciplinary action up to, and including, termination of employment.

PROCEDURE

1. The Security Officer is responsible for ensuring the Corporate 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.

2. Harris Workforce Members are responsible for reviewing, understanding and adhering to this Corporate Information Security Management Program Policy and related information security policies and procedures.

3. Access Control
   Users must use their own unique ID (username) and an associated password to access information and systems. Workforce Members are strictly prohibited from sharing usernames and passwords. Access control is required to make sure users can only access the systems and information that they are authorized to. Access is also controlled by means like automatic locking or log off of systems when needed. Users must use encryption when sending, receiving or maintaining PHI, PII or other Sensitive Information. For additional information on Access Control refer to the Corporate Access Control Policy.

4. Asset Tracking
   Corporate IT (CIT) is responsible for asset management which is a process for deploying, maintaining, upgrading and disposing of assets in a controlled and cost-effective manner. Asset management also helps CIT to ensure that the most recent updates and patches are applied for the security of the assets and to help prevent the loss of information. Workforce Members are required to notify CIT and the Security Officer immediately upon discovering an asset has been lost or stolen. For additional information on Asset Management refer to the Corporate Asset Tracking Policy.

5. Back-Up, Device and Media Controls
   Acceptable types of media, proper management, disposal, re-use of and accountability for media is specified to ensure the security of Harris systems and information including backup storage procedures and legal requirements for using third party vendors for offsite storage. This ensures that computer equipment and electronic storage media that contain or can be used to access computer equipment and electronic storage media that contain PHI, PII or other Sensitive Information are monitored and PHI, PII or other Sensitive Information is disposed of in a secure manner. Controls are maintained for all hardware and software moving into, out of and within the Harris facilities. For additional information on Device and Media Controls refer to the Corporate Back-Up, Device and Media Controls Policy.

6. Change Control

Change control is a process to manage changes in the environment to ensure no unnecessary or detrimental changes are made, all changes are documented and communicated. This helps minimize service disruptions and ensures resources are used efficiently. Formal change control procedures are followed when implementing changes to information systems which includes oversight by the Change Advisory Board. For additional information on Change Control refer to the Change Control Policy and the Change Management Protocol.

7. Communications, Data Sharing and Storage
   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. It is the responsibility of Workforce Members to understand how to protect this information when communicating or sharing information to Workforce Members, contractors, vendors or customers. Appropriate uses of the various tools by which information may be communicated, stored or shared such as Instant Messaging, Email, Voice and Video Conferencing, Online Shared Drives, etc. is defined in more detail in the Corporate Communications, Data Sharing and Storage Policy.

8. Configuration Management Policy
   Configuration management guidelines are established in order to help with managing risks associated with system or infrastructure changes. The configuration management guidelines are to be followed as closely as possible to ensure the security of Harris systems and data. When new systems are introduced or changes are to be made to existing systems or infrastructure, a process of documentation, specification, testing, quality control, configuration guidelines and managed implementation will be followed. Minimum requirements and guidance for baseline configuration of systems and resources that are implemented through a change control process are defined in the Corporate Configuration Management Policy.

9. Data Incident
   Data incidents are any suspected or actual impermissible use or disclosure, security incident, breach of PHI or PII. All Workforce Members, contractors and Business Associates must report any information regarding Data Incidents as quickly as possible to the Security Officer (Security_Officer@harriscomputer.com) or the Privacy Officer (Privacy_Officer@harriscomputer.com). If the Security Officer or the Privacy Officer is not available, the individual must report the issue to the Director of CIT or General Counsel. Workforce Members are made aware of their responsibilities during training and should refer to the Corporate Data Incident Policy for additional information.

10. Disaster Recovery and Business Continuity

Harris maintains an Information Technology Disaster Recovery and Business Continuity Program (IT DR\BC). The IT DR\BC Program prescribes that CIT and participating business units will have individual IT DR\BC Plans that include procedures for responding to an emergency, disaster or other occurrence that damages systems and/or applications which interrupts business operations. For additional information on IT DR\BC refer to the Corporate Disaster Recovery and Business Continuity Policy.

11. Email Policy
Harris email services are provided to staff for legitimate Harris-related activities. Inappropriate use of Harris email is strictly prohibited. Harris reserves the right to inspect, copy, store or disclose the contents of any email sent from any Harris user, if required and as appropriate. Users of Harris' email system consent to all provisions of the Corporate Email Policy. The Corporate Email Policy describes appropriate use and access of Harris email, email retention and disposal, and procedures for reporting spam or other email related malicious activity. For additional information refer to the Corporate Email Policy.

12. Facility Access Control Policy
To ensure the protection of staff as well as Harris systems and information, secure access to facilities are established according to the Facility Access Control Policy. Harris' information systems must be physically located where unauthorized access is minimized and an appropriate level of protection of the systems are provided. An assessment of physical access controls and risks are to be performed. Access to facilities are documented and logs are reviewed regularly. Environmental and physical protection of systems and information using controls such as redundant power supplies, fire suppression, etc. is also specified. Please refer to the Corporate Facility Access Control Policy for additional information.

13. Incident Response Plan
Security incident response processes are documented to address and manage activities during and after a security breach. The goal of security incident response is to handle the situation in an organized and effective manner that limits damage to the organization and reduces recovery time and cost. The Security Incident Response Plan provides guidelines on what constitutes an incident, along with a process that must be followed when a security incident occurs. Refer to the Corporate Incident Response Plan for additional information on the steps to take in the event of a security incident.

14. Information Access Management Policy
Access to PHI, PII or other Sensitive Information is to be granted only to Workforce Members who require the information to accomplish the work responsibilities of their position and is to be granted on a minimum necessary or need-to-know basis. Business associate agreements, non-disclosure agreements or other agreements as appropriate must be in place prior to non-Harris user or system access being granted to information or systems that contain PHI, PII or other Sensitive Information. The Governance, Risk and Compliance Committee (GRCC) to ensures that access rights to Harris information systems containing PHI, PII or other Sensitive Information is periodically reviewed and are appropriately granted.

Refer to the Corporate Information Access Management Policy for additional information on appropriate access and procedures on how access is to be established or modified, including account access during employee on-boarding and termination.

15. Mobile Device Usage Policy
    Harris users who use approved personal mobile devices will maintain specific protections and precautions to reduce the potential exposure of PHI, PII or other Sensitive Information. CIT is responsible for configuring and supporting the user's mobile device access to Harris computing resources to include the ability to remote wipe Company data when appropriate. Users are responsible for using Harris computing resources on his/her personal mobile device within the same constraints as on a Company-owned device to include password protecting the mobile device, keeping the device current with security patches and updates and abiding by the responsibilities outlined within the Corporate Mobile Device Usage Policy.

16. Network Management Policy
    Network management helps control network access and ensure the security of systems and data on the network. Harris' network and all devices must be securely managed to protect against threats, maintain security of systems and applications and information in transit. All network services security features, services levels, and management requirements are defined in network services agreements. Refer to the Corporate Network Management Policy for additional information.

17. Password Policy
    Passwords are the front line of defense for user accounts. Using strong passwords and changing them often are two ways to guard them from being guessed by a malicious user. All system-level passwords must be changed quarterly, and are maintained in a secure database by CIT. All user level passwords must be complex, a minimum of eight (8) characters, and changed every 90 days. Passwords should not be shared with anyone, written down or accessible in anyway by an unauthorized user. Appropriate use and management of passwords is detailed in the Corporate Password Policy.

18. Portable Computing Devices Policy
    Only Harris approved portable computing devices such as laptops, tablets, smartphones, etc. may be used for business purposes. Approval and verification of device configuration by CIT is required for use of a personally owned computing device prior to connecting to the Harris network, servers or workstations. PHI, PII and other Sensitive Information may not be stored on Portable Computing Devices unless the device is encrypted and the device is password protected. In the event a device used for Harris business purposes is lost or stolen it must be reported immediately. Security precautions must be followed such as using strong passwords, encryption, etc. when using portable devices for Harris business. Refer to the Corporate Portable Computing Devices Policy for additional information on when the use of portable devices is appropriate and how to securely use them.

19. Protection from Malicious Software Policy

All Harris' systems must be protected from malicious software (i.e. viruses, worms, etc.) by approved anti-malware software. Anti-malware software must be regularly updated and active at all times. This applies to both Harris owned computers and approved personally owned computers attached to a Harris owned network. Any activity intended to create and/or distribute malicious programs onto any Harris network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited. Any infected computer must be removed from the network until it is verified as infection-free. Workforce Members should contact CIT immediately if they encounter activity or correspondence that is believed to be malicious. Workforce Members must be cautious when accessing files, email and other resources that could potentially be harmful. Please refer to the Corporate Protection from Malicious Software Policy for additional guidelines and procedures on protecting Harris' systems and information from malicious software and activity.

20. Remote Access Policy
Connecting to the Harris network from a remote location outside of the private network may expose Harris to unwanted threats. Remote access to Harris systems or networks with PHI, PII or other Sensitive Information will be granted only as necessary and access will be reviewed periodically. All Remote Users working with Confidential Information, Sensitive Information, PHI or PII must use Harris' VPN services for remote access. It is the responsibility of Remote Users to ensure that their remote access connection is given the same consideration as the User's on-site connection to Harris. Each Remote User is responsible for safeguarding their password and User ID and protecting them from unauthorized use. Remote Users must ensure that Harris owned or approved personally owned computers, which are remotely connected to Harris' network, are configured to comply with Harris Security Policies and are protected with the latest malware software protection

before making a connection to the Harris network. Refer to the Corporate Remote Access Policy for detailed information on the policy and guidelines for remote access to the Harris network.

21. Responsible Use of IT Resources Policy
Workforce Members must use Harris IT resources responsibly and for approved business purposes. Users will be provided with access to various systems and information based upon their individual role and need. Users are responsible for all activity performed with their personal User-IDs. User-IDs may not be used by anyone but the individuals to whom they have been issued. Passwords must meet the guidelines and be used according to the Corporate Password Policy. The use of Harris IT resources for any illegal or inappropriate activity is strictly prohibited. There is no expectation of privacy of information on Harris owned IT resources or as it passes through Harris' network. Users must not use Harris IT resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by Harris management. Unless specified otherwise by contract, all confidential or proprietary information, must be protected and may not be shared or removed outside of Harris unless there has been prior

written approval. Refer to the Corporate Policy for Responsible Use of IT Resources for additional information on the appropriate use of Harris IT resources.

22. Risk Assessment and Analysis
    The Security Officer in conjunction with the Governance, Risk and Compliance Committee (GRCC), key management staff and the IT Department shall 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 shall 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 shall be engaged at least once every three years. For additional information refer to the Risk Assessment and Analysis Policy.

23. Security Awareness and Training Program
    Harris maintains a Security Awareness and Training Program for all Workforce Members to ensure an understanding of their roles and responsibilities. The Security Officer in conjunction with Human Resources (HR) and the Governance, Risk and Compliance Committee (GRCC) will ensure that the Security Awareness and Training Program is uniformly delivered to all new Workforce Members within 90 days of employment, as well as all Workforce Members at least annually. 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. Security Policies and Procedures will be reviewed and updated with any new technology and practices on an annual basis. Training materials will be updated to reflect any new or amended Security Policies and Procedures. Refer to the Corporate Security Awareness and Training Policy for additional information.

24. Security Management Policy
    Information security is managed through processes to identify risks that may impact Harris systems or information and the adoption of reasonable and appropriate measures to reduce any risks and vulnerabilities. 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. Technical, physical and administrative controls are implemented to ensure the integrity of PHI, PII or other Sensitive Information as appropriate. The Security Officer is responsible for ensuring Harris' Information Security 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. Refer to the Corporate Security Management Policy for additional information.

25. Security Risk Assessment Policy
    Risk or vulnerability assessments are conducted regularly for applicable businesses

to identify potentials risk or vulnerabilities that may negatively impact systems or information. The Security Officer works with key staff to address findings from the assessments to address security risks or vulnerabilities and to meet regulatory requirements. All assessment findings, remediation options, recommendations and remediation decisions are documented and maintained by the Security Officer. Refer to the Corporate Security Risk Assessment Policy for additional information.

26. Transmission Security Policy
    When sending PHI, PII or other Sensitive Information over an electronic communications network, it must be sent in encrypted form to safeguard the integrity of the data. Harris instant messaging is not encrypted and therefore PHI,

    PII or other Sensitive Information should not be sent via instant messaging or instant messaging attachments. Email sent externally is not encrypted by default, therefore all email or email attachments containing PHI, PII or other Sensitive Information must be sent using standard encryption processes. If the ability to encrypt is not available or if there is uncertainty that the communication is encrypted, the user must contact CIT prior to corresponding using PHI, PII or other Sensitive Information. At no time, should any member of the workforce use any email domains or instant messaging system other than their work email or instant messaging system (i.e., no public email domains such as gmail, yahoo accounts, etc.) to send PHI, PII or other Sensitive Information. Secure VPN is used to connect remotely to the network and encryption is used to transfer files (sFTP) or send sensitive email. For additional information on securely transmitting information refer to the Corporate Transmission Security Policy.

27. Workstation Use and Security Policy
    Harris issues workstations to Workforce Members with the expectation that it will be used for business purposes only. Workforce Members may not use the workstation to engage in illegal or inappropriate activity. Any personally owned computer used for Harris business local or remotely must be reviewed and approved by CIT prior to connecting to Harris' network. When Workforce Members leave the Company, their privileges, both internal and remote, are disabled or removed by the time of departure. Access to all Harris owned computers containing PHI, PII or other Sensitive Information is controlled by reasonable and appropriate authentication methods. Users must at a minimum lock their computers when not occupying it. Users must log off from or lock their computer(s) when their shifts are complete. Refer to the Corporate Workstation Use and Security Policy for additional information.

COMPLIANCE

Anyone found to have violated this policy is subject to disciplinary action, up to and including termination of employment, termination of contract and/or expulsion.