HARRIS COMPUTER SYSTEMS

CORPORATE NETWORK MANAGEMENT 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	Minor	Annual Review, Inserted Wireless Access and Network Access control statements	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual, 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 network access by using appropriate authorized tools, utilities and processes that supports secure network management. Harris' network and all devices are 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 clearly defined in network services agreements and are periodically audited.

PROCEDURE

1. Network Device Configuration
   a. Automatic network-based identification of equipment will be used as needed and appropriate using industry standards and best practices.
   b. Where additional security measures need to be applied, port-level restrictions will be used as needed and appropriate using industry standards and best practices.
   c. A multi-tiered network topology segregating development, testing, operational and other environments will be used as needed and appropriate using industry standards and best practices.
   d. Network devices including routers, firewalls, switches, etc. are managed, configured, tested and physically secured as needed and appropriate using industry standards and best practices.
   e. Network device configurations are appropriately documented and maintained.
   f. Network devices are configured to deny or control any unauthorized traffic into Company networks or devices used to conduct Company business.

2. Wireless Access
   a. Wireless access to systems and data is managed using network access control that authenticates systems and users as appropriate.
   b. Prior authorization by the VP of IT or designee is required for wireless access point implementation and connectivity to Company networks.
   c. Wireless access points are configured with industry standard encryption technology to protect systems and data where appropriate.
   d. Wireless access point vendor defaults such as encryption keys and passwords are changed prior to authorizing the implementation of the access point.
   e. Wireless access points are placed in physically secure locations that are restricted to only those authorized.
   f. File Sharing with non-Harris networks is restricted to only secure CIT supported file sharing capabilities (i.e., secure file transfer protocol (sFTP). Refer to the Corporate Communications, Data Sharing and Storage Policy for additional information.
   g. MAC address authentication and static IP addresses are implemented for wireless access points where appropriate.

3. Network Maintenance
   a. Network devices including routers, firewalls, switches, etc. are managed, configured, updated and physically secured as needed and appropriate using industry standards and best practices.

4. Network Monitoring
   a. Network devices including routers, firewalls, switches, intrusion detection devices, etc. are monitored for appropriate functionality and access as needed and appropriate using industry standards and best practices. Including Intrusion Detection System and Intrusion Prevention System (IDS/IPS) alerts are used for reporting information security events.
   b. Network Access Control is used to monitor systems for compliance of to security patches and anti-virus definition requirements prior to being authorized to access Company or guest networks.
   c. NAC permits only Company authorized systems onto Company networks.
   d. NAC is used to identify unauthorized devices or wireless access points and to generate alerts for appropriate response.

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)