HARRIS COMPUTER SYSTEMS

CORPORATE REMOTE ACCESS POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/8/16	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 section re: Remote Access to Customers or Third Parties, Right to audit remote user's home work space.	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

Harris Computer Systems
Remote Access Control Policy

POLICY

Harris Computer Systems (Harris or Company), maintains standards for connecting to the Harris network from remote locations outside the private network. The standards are designed to minimize the potential exposure to Harris from threats that may result from unauthorized use of Harris resources or unauthorized exposure to Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information. Harris shall maintain secure mechanisms for remote access to PHI, PII or other Sensitive Information.

SCOPE

This policy applies to all Users including but not limited to Workforce Members, contractors and vendors who connect remotely to the Company's network or systems ("Remote Users"). This policy applies to remote access connections used to conduct Company business, including but not limited to, receiving or sending e-mail and viewing intranet Web resources. All remote access implementations to Company network or systems are covered by this policy including but not limited to frame relay, ISDN, DSL, VPN, SSH, cable modems, and hardware or services provided by third parties.

PROCEDURE

1. Remote access to Company systems or networks with PHI, PII or other Sensitive Information shall be granted only as necessary. Such grants of access are reviewed periodically and may be revoked at any time for failure to comply with the requirements of this policy. If a Remote User (other than a Workforce Member) will be given access to PHI, PII or other Sensitive Information, a Business Associate Agreement between the Company and the Remote User is required and the Business Associate Agreement must be in place before granting remote access. Refer to the Information Access Management Policy.

2. 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 the Company network. See the Network Management Policy, Responsible Use of IT Resources Policy, Access Controls Policy, Information Access Management Policy and Workstation Use and Security Policy.

3. Remote Users must comply with federal, state/provincial, and local law and all Company policies.

4. All Remote Users working with Confidential Information, Sensitive Information, PHI or PII must use the Company's VPN services for remote access. Remote Users may not use hotel, library or other public workstations and Wireless Access Points (WAPs) when working with PHI, PII or other Sensitive Information without the use of secure VPN.

5. Each Remote User is responsible for adhering to the Corporate Password Policy and safeguarding his or her password and User ID to protect them from unauthorized use. Remote Users are prohibited from providing their password or User IDs to anyone else, for any reason. Compromised passwords and/or User IDs must be immediately changed.

6. Remote Users are responsible for ensuring that family members or household visitors do not gain access to the Company network, its resources or its data. Remote Users bear responsibility for any consequences arising from improperly protected User IDs and passwords or remote access misuse or misappropriation. When working with PHI, PII or other Sensitive Information Remote Users must use an area that is not easily accessible by other household members, provides a lockable cupboard/cabinet for storing portable equipment when not in use, is not easily viewable/accessible from the outside. Harris has the right to audit a home work space including requesting a photograph of the area, using a web cam to view the workspace in real time, or (in high risk cases) a visit to the person's home office.

7. Any unauthorized attempt to discover the password of another User or to access Company information or systems using another person's password or user ID is prohibited.

8. Remote Users must ensure that any computer or workstation, which is used to remotely connect to the Company's network, is not connected to any other network at the same time, other than a Private Network under the Remote User's control.

9. Remote Users must ensure that Harris owned or CIT approved personally owned computers, which are remotely connected to the Company's network, are configured to comply with Information Security Management Program and associated policies and procedures and are protected with the latest malware software protection before making a connection to the Company network. Remote Users are responsible for keeping malware definitions up to date, running regular anti-malware scans and ensuring security patches are up to date. If a Remote User fails to meet these standards, remote access will be denied or revoked. See Protection from Malicious Software Policy.

10. Remote Users must not use non-Company email accounts (i.e., Hotmail, Yahoo, AOL, Google mail), or other external resources to conduct Company business, thereby ensuring that official business is never confused with personal business. For the purpose of best practice, Workforce Members should not use customer assigned email accounts for Company business without prior written manager approval.

11. Remote Users who wish to implement non-standard hardware configurations for remote access to Company network or systems must obtain prior approval from Corporate IT. All authorized remote access will be centrally managed by Corporate IT and will use strong authentication measures.

12. Multifactor Authentication – The Company has instituted Multifactor Authentication for Remote Users to access Company network or systems.

ADDITIONAL THIRD PARTY ACCESS REQUIREMENTS

External Company network connections to Harris can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the Company network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts. Therefore, all external network connections required to connect to a Harris network must be established through a secure tunnel that is approved by Corporate IT. This policy applies to all new third-party network connection requests and any existing third-party network connections. All third-party network connections must meet all of the guidelines and requirements outlined in this policy.

1. Contractor Access

   In addition to the above requirements, Contractors must ensure that all Company Confidential Information is protected from inadvertent disclosure when being sent over the Internet or other open, non-Company networks. Encryption must be used to protect Company Confidential Information. If unable to encrypt, Contractors should consider alternatives to email for transference.

2. Vendor Access

   In addition to the above requirements, Vendor remote access must be uniquely identifiable and password management must comply with the Corporate Password Policy. Vendor's major work activities must be entered into a log and available to Harris management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

   Upon departure of a vendor's employee from the contract for any reason, the vendor will ensure that: (i) all Confidential and other Sensitive Information is collected from the employee and returned to the Company or destroyed within 24 hours; (ii) all PHI and PII is collected from the employee and returned to the Company or destroyed in accordance with the Business Associate Agreement entered into by Harris and the Vendor; and (iii) the employees remote access to the Harris' network or systems is terminated immediately.

Upon termination or expiration of the applicable contract or at the request of the Company, the vendor will return or destroy all Company information (including Confidential Information, PHI, PII and other Sensitive Information) and provide written certification of that return or destruction within 24 hours and terminate any remote access immediately. All User IDs and passwords used for remote access to Harris systems or network must be deactivated immediately.

Upon termination or expiration of contract or at the request of Harris, the vendor must surrender all Company identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Harris management.

Vendors are required to comply with all state, federal/provincial and Harris auditing requirements, including the auditing of the vendor's work.

All software used by the vendor in providing service to Harris must be properly inventoried and licensed.

3. Harris' Remote Access to Customers or Third Parties

   Workforce Members must only access customers or third parties for a business need as authorized by the customer or third party. Workforce Members must ensure that all Company Confidential Information, PHI, PII or other Sensitive Information is protected from inadvertent disclosure when being sent over the Internet or other open, non-Company networks. Encryption must be used to protect Company Confidential Information, PHI, PII or other Sensitive Information. Workforce Member remote access to customer or third-party networks must be uniquely identifiable and password management must comply with the Company Password Policy.

4. Third Party Access to Company Systems

   For all system connections that allow third parties to access the Company's computing assets such as Web Sites, portals, kiosks and public access terminals, the Company provides appropriate text or a link to the Company's privacy policy for data use and protection as well as the third party's responsibilities when accessing the data.

REMOTE ACCESS METHODS

1. Routers for dedicated communications lines configured for access to the Company network must meet minimum authentication requirements of the Challenge Handshake Authentication Protocol (CHAP).

2. Frame Relay must meet minimum authentication requirements of the Data Link Connection Identifier (DLCI) standards. The DLCI is a unique number assigned to a permanent virtual circuit (PVC) end point in a frame relay network. DCLI identifies a particular PVC end point with a user's access channel in a frame relay and has local significance only to that channel.

3. VPN User Managed Service: the User is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing any required software. The following guidelines apply to VPN:

    a) VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

    b) When actively connected to the Harris network, VPNs will force all traffic to and from the Remote User's computer over the VPN tunnel: all other traffic will be dropped.

    c) Dual (split) tunneling is permitted via only Company authorized VPN access points.

    d) VPN gateways will be set up and managed by Corporate IT.

    e) Only Company-approved VPN clients may be used.

    f) Multi-factor authentication for remote access is used when applicable.

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.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

45 C.F.R. § 164.308(a)(4)

Harris Computer Systems
Remote Access Control Policy

45 C.F.R. § 164.312(d)