HARRIS COMPUTER SYSTEMS

CORPORATE COMMUNICATIONS, DATA SHARING AND STORAGE POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	5/6/2020	Katie Rose	Major	Initial version of policy.	Dwayne Martin
1.1	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

Harris Computer Systems
Corporate Communications, Data Sharing and Storage Policy

POLICY

Harris Computer Systems (Harris) is committed to controlling, managing and monitoring access to Electronic Protected Health Information (PHI), Personally Identifiable Information (PII), or other Sensitive Information by ensuring that it is communicated, shared and stored with appropriate safeguards and only when there is a legitimate business need.

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, customers or other Workforce Members. This policy defines 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. Refer to the Corporate Access Controls Policy for more information on appropriate access to information.

1. COMMUNICATIONS

a. Instant Messaging

i. Only Harris supported Instant Messaging (i.e. Teams, Skype for Business, etc.) are to be used for company related communications.

ii. Instant Messaging may be used for sharing or storing of data that is publicly consumable.

iii. Sharing or storing PHI, PII or other Sensitive Information via Instant Messaging tools is strictly prohibited.

iv. Access to Teams Channels and Meetings provided to non-Harris users may be granted by only an identified authorized user's email address such as a customer email address. If a public domain email account (i.e., gmail.com, yahoo.com, etc.) is used, it must be associated with an identified authorized user who is verified by the Team owner.

v. Allowing permission for non-Harris users to control Harris' workstations must be for a legitimate business need. The screen control session must be attended by the Workforce Member for the entire session. The Workforce Member will be accountable for all of the activity conducted from that system during the control session.

vi. When creating Teams Channels, access controls must be configured to ensure only authorized users have access to them.

b. Email Messaging

i. Harris email communications must be via Harris supported email messaging tools (i.e. Outlook Client or Outlook via Office 365).

ii. Transmission via email of PHI, PII or other Sensitive Information is discouraged. If there is a legitimate business need and no other secure means for sending PHI, PII or other Sensitive Information outside of Harris network,

the email must be limited to the minimum necessary, sent only to authorized recipients and encrypted. Refer to the Corporate Email Policy for additional information.

c. Voice and Video Conferencing

i. Various tools are used for voice and video conferencing (i.e. Teams, Skype for Business, WebEx, etc.). Appropriate data protection standards must be followed during a voice or video conference that involve PHI, PII or other Sensitive Information.

ii. Information shared via voice or video conferencing must be limited to intended authorized individuals and limited to minimum necessary.

iii. Screensharing must be limited to only those authorized and may not include PHI, PII or other Sensitive Information.

d. Customer and Vendor Communications

i. Customer support systems may be used to interact with customers (i.e. CRM, JIRA, etc.). These systems must have security controls to protect customer data such as appropriate access controls and encryption in transit and at rest.

ii. Users who join voice or video conferences organized by customers or vendors must ensure that the communication and information shared is limited to intended authorized individuals and limited to minimum necessary.

2. DATA STORAGE AND SHARING

a. Internal Online Shared Drives

i. Internal Online Shared Drives (i.e., OneDrive for Business assigned to workforce members) are file shares that are accessible via a secure network connection using authorized Harris issued credentials. The file shares contain company data and are configured with appropriate access controls for authorized Workforce Members.

ii. Only Harris supported Online Shared Drive services (i.e., Harris OneDrive for Business) are to be used for Company related communications, data sharing and storage.

iii. Access to Internal Online Shared Drives may only be granted to authorized Workforce Members.

iv. Data Loss Prevention (DLP) policies are enforced for all Harris supported Internal Online Shared Drives to meet appropriate data security and compliance requirements.

v. Creation of Internal Online Shared Drives must align with the standards, security controls and naming conventions as outlined by Corporate Information Technology (CIT). Refer to CIT SharePoint Online and Teams Use and Configurations Guidelines for additional information.

b. External Online Shared Drives

i. External Online Shared Drives (i.e., Harris SharePoint Online) are secure file shares accessible via the Internet. The file shares are configured by Harris Workforce Members as the designated owner, who grant access to authorized external users as appropriate.

ii. The use of External Online Shared Drives for sharing any Company data with authorized non-Harris users is restricted to an appropriately configured SharePoint sub-site as described in the CIT SharePoint Online and Teams Use and Configurations Guidelines**.**

iii. The use of External Online Shared Drives established by a third party (i.e., during due diligence) is governed by the access granted by the third party. If an External Online Shared Drive is established by a Harris user to collect data from a third party, it must meet the guidelines within this policy.

iv. Storage of PHI on External Online Shared Drives is prohibited.

v. Storage of PII or other Sensitive Information must be the Minimum Necessary and must be removed from the secured storage when no longer needed.

vi. Access to External Online Shared Drives to authorized non-Harris users is granted to only an appropriate email address such as a customer email address.

vii. If access to External Online Shared Drives via a public domain email account (i.e. gmail.com, yahoo.com, etc.) is required, it must be associated by an identified authorized user who is verified by the shared drive owner.

viii. External sharing of Company data via Harris SharePoint Online must be Minimum Necessary, to only authorized non-Harris users and only for the required duration. If a public domain email account (i.e., gmail.com, yahoo.com, etc.) is used for external sharing, it must be associated with an identified authorized user who is verified by the Information Owner.

ix. The use of other external data sharing tools (i.e., DropBox, Google Drive, etc.) is prohibited.

x. Data Loss Prevention (DLP) policies are enforced for all Harris supported External Online Shared Drives to meet appropriate data security and compliance requirements.

xi. Creation of External Online Shared Drives must align with the standards, security controls and naming conventions as outlined by CIT. Refer to the CIT SharePoint Online and Teams Use and Configurations Guidelines for additional information.

xii. Any suspected breach of information shared or stored must be reported to the Corporate Information Security Officer or Privacy Officer immediately.

c. Internal Network Drives

i. Internal Network Drives of servers (i.e. Mapped Network Drives, On-Premise SharePoint) must be protected by firewalls and only accessible via the office network or a Harris Virtual Private Network (VPN) connection.

ii. Internal Network Drives of servers with appropriate safeguards must be used for storage and sharing of PHI, PII or other Sensitive Information.
iii. Sharing of Internal Network Drives of servers to any non-Harris user is prohibited.
iv. Sharing of information located on the internal network to external parties must be limited to the use of secure File Transfer Protocol (sFTP) servers that are appropriately patched and securely configured.

STANDARDS

1. General Communications
    a. Communications via Email, Instant Messaging, Voice and Video Conferencing must be limited to intended authorized individuals.
    b. Sending communications that contain PHI, PII or other Sensitive Information is discouraged. If there is a legitimate business need, the communications must be the Minimum Necessary, sent to only authorized recipients and encrypted.
    c. Information shared via voice or video conferencing must be limited to intended authorized individuals and minimum necessary.
    d. Users must be aware of attendee's capability to take screenshots and therefore should never display PHI, PII or other Sensitive Information when screensharing during a voice or video conference. If there is a potential for PHI, PII or other Sensitive Information to be displayed during a screenshare appropriate safeguards must be in place per the Corporate Workstation Use and Security Policy.

2. Data Storage
    a. PHI, PII or other Sensitive Information must be stored on secured servers with appropriate safeguards such as access controls, encryption, behind a firewall, etc.
    b. Periodic audits of all PHI, PII or other Sensitive Information data stored must be performed by the Information Owner to ensure security and access controls are appropriate, and that retention of the data is required. If the data is no longer required it must be deleted according to the Corporate Backup, Device and Media Controls Policy.
    c. Publicly consumable data (i.e. FAQ's, support documentation, etc.) may be stored on Harris supported Instant Messaging channels or External Shared Drives.
    d. PHI, PII or other Sensitive Information may never be stored via publicly accessible medium.
    e. The use of External Online Shared Drives for storage of PII or other Sensitive Information must be for only those authorized via appropriate access controls and removed when no longer needed.

3. Data Sharing
    a. PHI, PII or other Sensitive Information must be shared with only those authorized via secured servers with appropriate safeguards such as access controls, encryption, behind a firewall, etc.
    b. Sharing of PHI, PII or other Sensitive Information must be as Minimum Necessary, with appropriate access controls and via a secure method.
    c. Sharing of PHI via email must be the Minimum Necessary and is only permitted among authorized Workforce Members.

d. PHI, PII or other Sensitive Information may never be shared via any publicly accessible medium or unsecured method.
e. Sharing of PHI on External Online Shared Drives is prohibited.
f. The use of External Online Shared Drives for sharing of PII or other Sensitive Information must be Minimum Necessary and removed when no longer needed.

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)