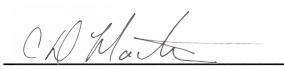
HARRIS COMPUTER SYSTEMS

CORPORATE RESPONSIBLE USE OF IT RESOURCES POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/13/15	Rick Martin	Major	Initial version of policy.	Dwayne Martin
1.1	08/17/15	Katie Rose	Minor	Updated format, referenced applicable policies.	Todd Richardson
1.2	10/22/18	Katie Rose	Minor	Annual Review	Dwayne Martin
1.3	3/25/2020 *2019 review waived as approval for 2018 review cycle completed end of Q1 2019	Katie Rose	Minor	Annual Review; renamed the document from Policy for Responsible Use of IT Resources to Responsible Use of IT Resources	Dwayne Martin
1.4	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

PURPOSE

This policy is designed to define the appropriate and responsible use of the information and technology resources at Harris including staff computing and network facilities. Each authorized user of information and technology resources must assume responsibility for

his/her own behavior while utilizing these resources. Users of information and technology resources at Harris must adhere to the same morality and ethical behavior guidelines in their computing and networking environment as is required in their non-computing environments.

SCOPE

This policy applies to all Workforce Member, contractors, subcontractors, vendors or any other individual using information technology at Harris ("User" or "Users"). Access to Harris owned computer facilities, equipment, hardware, software, printing services, cloud services and technology staff provided user support, is a privilege, not a right. Accepting access to this technology carries an associated expectation of responsible and acceptable use. When accessing any remote resources using Harris technology resources, Users are required to comply with both this policy and all applicable policies governing the use and access of the remote computer system. Refer to the Corporate Remote Access Policy for more information.

COMPLIANCE

All Users of Harris information and technology resources are required to comply with this policy and with all applicable local, state/provincial and federal laws and regulations. Harris reserves the right to amend this policy at any time and without prior notice. Harris reserves the right to deny, limit, restrict or extend computing privileges and access to its information and technology resources of any User at any time.

ACCESS & PRIVILEGES

1. User Accounts

Users will be provided with access to various information systems and technology based upon their individual role and need. User account access may include but is not limited to: individual computers or workstations, personal network file space, the Internet, the Harris Intranet, portals, web space, cloud based applications, email and telephone. Access to these accounts is a privilege not a right and may be revoked for any reason including non-compliance with this policy. See the Corporate User Access Control Policy for more information.

2. User-ID

Users are responsible for all activity performed with their personal User-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their User-IDs. Similarly, Users are forbidden from performing any activity with IDs belonging to other Users. Any suspected unauthorized access of a User account should be reported immediately to the Vice President of Corporate IT or the Information Security Officer.

3. Passwords

Regardless of the circumstances, Users must never share or reveal their password to anyone else, including but not limited to colleagues, management or family members. Violations of this prohibition can result in sanctions up to and including termination. Users will be responsible for any actions taken with their User-ID and password by any individual with whom they have shared or revealed their password. If Users need to share data located on their individual computer or workstation, they should use electronic mail, secure directories on local area network servers, and other Corporate IT approved mechanisms. All Users are responsible for both the protection of their User account password and the data accessible and secured with their User account. See the Corporate Password Policy and the Corporate Information Access Management Policy for more information.

4. System Privilege Deactivation

All Harris information systems privileges both internal and remote must be deactivated at the time that a User ceases to provide services to Harris. The time frame for deactivation may vary according to the needs of specific systems and are determined by procedures established by Corporate IT. All data, files, or messages are removed from User accounts when account deactivation occurs.

5. No Responsibility for Personally Owned Computers

Harris cannot provide, and will not be responsible for, software or data kept on personally owned computers, nor is it responsible for the installation, repair, maintenance or upgrade of personally owned hardware. Any personally owned computers used for Harris business, local or remote, must be reviewed and approved by Corporate IT prior to connecting to Harris networks. See the Corporate Portable Computing Devices Policy and the Remote Access Policy for more information.

6. Incidental Personal Use of Information Resources

Harris allows Users to make reasonable and incidental personal use of its electronic mail and other computer and communications systems. Incidental personal use is permissible if the use:

- Does not consume more than a trivial amount of resources that could otherwise be used for business purposes
- Does not interfere with worker productivity, and
- Does not pre-empt any business activity.

All such personal use must be consistent with conventional standards of ethical and polite conduct. For example, electronic mail must not be used to distribute or display messages or graphics, which may reasonably be considered by some to be disruptive or offensive (such as sexual jokes or pornography).

ACCEPTABLE USE

Harris Computer Systems
Corporate Responsible
Use of IT Resources Policy

1. Acceptable Uses of Information Technology or Systems

Harris information systems are provided to assist Users in acquiring and disseminating information related to the performance of assigned duties, roles and responsibilities. See the Corporate Workstation Use and Security Policy for more information.

2. Unacceptable Uses of Information Technology or Systems

Any information, data, or programs not consistent with the business of Harris must not be created, stored, transmitted, viewed or manipulated by Users using Harris owned technology or information systems. Users must not use Harris information, technology or information systems in the following manner:

- Transmitting any material, or engaging in any other activity in violation of any federal, state/provincial, or local laws, including copyright law.
- Transmitting or accessing information containing harassing material. Computer harassment includes, but is not limited to:
    - Sending or displaying text or images using technology or information systems with the intent to harass, terrify, intimidate, threaten or offend another person;
    - Intentionally using technology or information systems to contact another person repeatedly with the intent to harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
    - Intentionally using technology or information systems to disrupt or damage the work of another; or
    - Intentionally using technology or information systems to invade the privacy of another or to threaten the invasion of the privacy of another.
- Transmitting, receiving, displaying, viewing, printing or storing offensive content, which includes, but is not limited to:
    - Sexually explicit, obscene or pornographic comments or images;
    - Discriminatory comments or images including any comments or images that would offend someone on the basis of their age, sex, sexual orientation, race, color, national origin, religion, disability or health status;
    - Graphically disturbing comments or images; fraudulent comments or images;
    - Harassing, threatening or abusive comments or images.
- Disseminating or printing copyrighted materials, including computer files, articles and software, in violation of copyright laws
- Attempting forgery of email messages
- Transmitting or accessing any information or system for personal purposes that depletes network/system resources available for business purposes
- Physical or electronic interference with other computer systems Users
- Any other practice or User activity that, in the opinion of Harris management constitutes irresponsible behavior, promotes illegal activities, results in the misuse of computer resources or jeopardizes the operation or security of computer or network systems.

3. Prohibition Against Commercial Use of Information Resources

Harris Users must not use Harris information and technology resources for soliciting

business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by Harris management. Prohibited activity includes, but is not limited to operating a business, usurping business opportunities or soliciting money for personal gain.

PRIVACY AND DATA OWNERSHIP

1. Legal Ownership of Information Systems Files and Messages

Harris has legal ownership of the contents of all files stored on its computer and network systems as well as all messages transmitted via these systems. Harris reserves the right to access all such information without prior notice whenever there is a genuine business need.

2. No Responsibility for Monitoring Content of Information Systems

Harris reserves the right to remove any message, file, database, graphic, or other material from its information systems. At the same time, Harris has no obligation to monitor the information content residing on or flowing through its information systems.

3. Privacy Expectations and Information Stored on Harris Systems

At any time and without prior notice, Harris reserves the right to examine electronic mail, instant messages, personal file directories, hard disk drive files, and other information stored on Harris information systems. Similarly, at any time and without prior notice, Harris reserves the right to examine, monitor or remove any device attached, for any reason, to the Harris data network. This examination is performed to assure compliance with internal policies, to support the performance of internal audits and investigations, to comply with legal requirements such as a subpoena or court order, and to assist with the management and security of Harris information systems.

4. Disclaimer of Responsibility for Damage to Data and Programs

Harris uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, Harris maintains the authority to:

- restrict or revoke any User's privileges,
- inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and
- take any other steps deemed necessary to manage and protect its information systems.

This authority may be exercised with or without notice to the involved Users. Harris disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

5. Handling of Third Party Confidential and Proprietary Information

Unless specified otherwise by contract, all confidential or proprietary information, including software written by a third party that has been entrusted to Harris by a third party, must be protected as though it was Harris' confidential information.

6. Confidentiality of Harris Software or Documentation

All Harris generated programs, codes and related documentation is confidential and must not be taken elsewhere when an employee leaves the employ of Harris, or a consultant or contractor ends their engagement with Harris.

7. Removal of Sensitive Information from Harris Premises

Confidential Harris information, no matter what form it happens to take, must not be shared with those outside of Harris, or removed from Harris premises, unless there has been prior written approval.

INTELLECTUAL PROPERTY

1. Copyright Laws

Unless placed in public domain by its owners, copyright laws protect software programs and other types of media such as audio files, videos and pictures. Software and other media types are also protected by the license agreements between the owner and purchaser. It is illegal to duplicate, copy, download or distribute software, other media types or its documentation without the permission of the copyright owner.

2. Software

Harris strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet Users or other system Users make unauthorized copies of software, the Users are doing so on their own behalf, since all such copying is strictly forbidden by Harris. Users should consult with Corporate IT prior to installing software on their computer.

3. Fair Use

Unless permission from the copyright owner(s) is first obtained, making copies of any material subject to a copyright including magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

PRIVACY

1. Financial, Health and Nonpublic Personal Data

Security and confidentiality are matters of concern to all Harris employees who have access to financial, health and nonpublic personal information either by hard copy documents or via electronic media. Harris is responsible for the accuracy, integrity and confidentiality of such electronic information. All electronic data must be treated as confidential, other than data that has been authorized for release to a third party. Since conduct, either on or off the job, could affect or threaten the security and confidentiality of this information, each employee who accesses administrative systems is required to adhere to the following:

- No one shall make or permit unauthorized use of any information in files

maintained, stored, or processed by any Harris information system.

- No one is permitted to seek personal benefit, allow others to benefit personally or to divulge, in any way, the contents of any record or report, to any person except in the conduct of his/her work assignment.
- No one shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry.
- No one shall knowingly change or delete or cause to be changed or deleted an entry in any record or report, unless expressly authorized to do so and in accordance with Harris policies and procedures.
- Once information is downloaded, data should not be altered in word processing documents or spreadsheets in a way that misrepresents the information derived from these data. Downloaded information should be used and represented responsibly.
- No record or report, or copy thereof, shall be removed from the Harris facility where it is maintained or copied or printed via electronic means except in the authorized performance of a person's duties, and in accordance with established procedures. Copies made in the performance of a person's duties shall not be released to third parties.
- No one is to aid, abet or act in conspiracy with another to violate any part of this policy.
- Any knowledge of a violation of this policy must immediately be reported to the employee's supervisor, the Vice President of Corporate IT or the Privacy Officer. Any reports shall be made free of concerns of retaliation. Any attempt to retaliate against a person for making a report regarding Harris' privacy practices will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment. Harris shall not intimidate, threaten, coerce, discriminate against or take any other retaliatory action against any individual for voicing a concern or complaint.
- All Users will activate workstation locking software whenever they leave their workstation unattended. All Users must log off from or lock their workstation(s) when their shifts are complete.

2. When Making Copies of Software is Permissible

Third party software in the possession of Harris must not be copied unless such copying is consistent with relevant license agreements and either:

- Corporate IT has previously approved of such copying, or
- Copies are being made for contingency planning purposes.

3. Access to Data

All access to Harris data must be approved by the appropriate Manager, Director or GM. Approval of access to the data consents to the use of these data within the normal business functions.

Access to data shall not be granted to persons unless there is an established business need to know. See the Corporate Information Access Management Policy for more information.

4. Violation of Access Privileges

Information Owners reserve the right to determine appropriate use of the data under his/her control. Usage violations may result in revocation of a User's access to the data.

DEFINITIONS

See attached policy definitions or click here.