




HARRIS

HARRIS COMPUTER SYSTEMS CORPORATE PROTECTION FROM MALICIOUS SOFTWARE POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	1/21/16	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	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

PURPOSE

The purpose of this policy is to define responsibility for malware control and to establish appropriate safeguards to protect Protected Health Information (PHI), Personally Identifiable Information (PII), other Sensitive Information, systems and other electronic information resources from malicious software including but not limited to viruses, worms, spyware and Trojan Horses. This policy is also intended to ensure that the effects or transmission of malicious software to systems or data does not damage the Harris Computer Systems (Harris) reputation.

SCOPE

This policy applies to all computers that are connected to Harris' network via a standard network connection, wireless connection, modem connection, or virtual private network connection or are used to connect to Harris Computing Resources. This includes both Harris owned computers and approved personally owned computers attached to a Harris owned network or used to access Harris Computing Resources. Harris Computing Resources include any Corporately provided service or application. The definition of computers includes desktop workstations, laptop computers, mobile devices and servers. All Workforce Members and users are subject to this policy and required to abide by it.

POLICY

1. Harris uses next-generation antivirus (NGAV) and endpoint detection and response (EDR) software for all systems that connect to Harris network.
2. All computers attached to any Harris owned network must run CIT approved and supported NGAV and EDR software. This antimalware software must be active at all times and must be configured to perform real-time checks on all executed files and scheduled malware checks at preset regular intervals. The malware definition files, and scan engines must be kept up to date at all times.
3. Each of the requirements listed above are controlled by CIT via CIT's antimalware management server and services and cannot be changed by Workforce Members.
4. 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.
5. If a Workforce Member receives what he/she believes to be malware, or suspects that a computer is infected with malware, he/she must report such incident to CIT using one of these contact methods: WEB: Submit a CIT

request via the portal <https://harriscomputer.my.salesforce.com/>, EMAIL: itrequest@harriscomputer.com, PHONE: Toll-Free 888-808-0960 or 613-696-0128. Report the following information (if known): malware name, extent of infection, source of malware, and potential recipients of infected material.

6. Any infected computer must be removed from the network immediately until it is verified as infection-free.

GUIDELINES

Responsibilities of Workforce Members

All Workforce Members and Users of Harris systems must take the following measures to guard against, detect, and reporting malicious software:

1. Not attempt to either alter or disable antimalware software installed on any computer attached to a Harris owned network without the express consent of CIT.
2. Never open files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
3. Never open files or macros attached to an email from a known source (even a coworker) if you were not expecting a specific attachment from that source.
4. Be suspicious of email messages containing links to unknown websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. The Harris' email system scans attachments for malware infections and blocks infected attachments from being transmitted to client systems.
6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
7. Avoid direct disk sharing with read/write access. Always scan any removable media for malware before using it.
8. If instructed to delete email messages believed to contain a malware be sure to also delete the message from your Deleted Items folder.
9. Back up critical data and systems configurations on a regular basis and store

backups in a safe place.

10. Never use personally owned computers or devices for Harris business purposes until CIT approved antimalware software is properly installed and it is properly updated (including installing recommended security patches for the operating system and other applications that are in use).
11. If a personally owned computer or device becomes infected by malware, the Workforce Member is responsible for the cleanup and removal of the malware.

Responsibilities of CIT

1. CIT is responsible for maintaining and updating this Protection from Malicious Software Policy. Copies of this policy will be posted on CIT's policy site.
2. CIT will keep the malware prevention products it provides up to date in terms of both malware definitions and software version in use. CIT's antimalware management server checks for updates in real-time auto updates both the malware definitions file and the software version on all client systems. The success or failure of the application's updates on clients is reported back to the management server or service. CIT will invest adequate efforts to identify client systems that did not attempt to update their malware definitions files and will take appropriate remedial actions.
3. CIT will apply any updates to the services it provides that are required to defend against threats from malware.
4. CIT will address false positives to determine the potential impact on the availability of information systems and take steps as appropriate.
5. CIT will install antimalware software on all Harris owned desktop workstations, laptops, and servers.
6. CIT can assist Workforce Members in installing antimalware software according to standards on CIT approved personally owned computers that will be used for business purposes. It will be at CIT's discretion whether antimalware software is provided in these cases. Workforce Members may not use personally owned computers for Harris business purposes unless antimalware software is properly installed and updated and has been approved by CIT.

7. CIT will take appropriate action to contain, remove, and assist in recovery from malware infections. In order to do so, CIT may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
8. CIT will check the management server logs on a daily basis for detected malware that are not quarantined by the antimalware software and take appropriate remedial actions.
9. CIT will attempt to notify Users of Harris systems of any credible malware threats. Malware reports will not be acted upon until validated. Workforce Members should not forward these or any malware warning messages in order to keep network traffic to a minimum.

DEFINITIONS

See attached policy definitions or [click here](#).

REGULATORY REFERENCES

45 C.R.F. §164.308(a)(5)(ii)(B)