IT6

Category: Information Technology

Anti-Malware POLICY

I. PURPOSE

The purpose of this policy is to set minimum standards for Pioneer's requirements for dealing with computer viruses, worms, Trojan Horses, spyware, Ransomware, and other types of malicious software.

II. SCOPE

This policy applies to all Pioneer employees that use Pioneer Information Systems.

III. DEFINITIONS

"Information Systems" shall mean an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.

"Malware," or "malicious software", means software that is designed to damage, disrupt, or abuse an individual computer or an entire network and/or steal or corrupt an organization's most valuable and sensitive data. Viruses, worms, and Trojan horses are examples of malware.

IV. POLICY

Pioneer information technology (IT) staff, in coordination with Pioneer's contracted managed services provider (MSP), shall ensure:

- Procedures and tools exist to guard against, detect, and report malicious software.
- IT personnel are trained and proficient in the use of the security solutions used to protect against malicious software.
- End users are aware of the security policies enforced on their workstations.
- Anti-virus software is installed at appropriate locations within organizational Information Systems including all systems commonly affected by malicious software.

Adopted: December 16, 2021
Resolution 2021-46

- Installed endpoint protection programs are capable of detecting, removing, and protecting against all known types of malicious software.
- Endpoint protection mechanisms are properly maintained and kept current with updates.
- Real time scan of files from external sources are performed as files are downloaded, opened, or executed.
- Endpoint protection mechanisms are actively running and cannot be disabled or altered by users.

All workstations whether connected to Pioneer's network, or standalone, must use Pioneer's approved virus protection software and configuration.

The protection software must not be disabled or bypassed.

The settings for the malware protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the malware protection software must not be altered to reduce the frequency of updates.

Each file server attached to Pioneer's network must utilize the Company's approved malware protection software and setup to detect and clean malware that may infect file shares.

Every malware that is not automatically cleaned by the virus protection software constitutes a security incident and the affected staff person is to report the incident to the IT staff.

Anti-malware signature updates shall be properly maintained by IT staff. Malware actions (e.g. anti-malware software updates, definition updates, malware infections, Ransomware attacks, etc.) shall be logged with logs retained for 100 days to allow proper investigations into malware related incidents.

V. ENFORCEMENT

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. DISTRIBUTION

This policy is to be distributed to all Pioneer staff who use Information Systems.