IT12
CATEGORY: INFORMATION TECHNOLOGY

MALWARE DEFENSE POLICY

I. PURPOSE

Prevent data loss, corruption, or misuse of Central Coast Community Energy (CCCE) computing resources or information that may occur when malware is introduced to CCCE's IT systems and services.

II. SCOPE

This policy applies to all CCCE personnel and to all computer hardware and software comprising CCCE's IT network.

III. DEFINITIONS

"**Malware,**" short for "**malicious software,**" is designed to damage, disrupt, or abuse an individual computer or network and/or steal or corrupt an organization's most data. Viruses, worms, and key loggers are examples of malware.

"**Spam or junk email**" are commercial email sent in bulk over the Internet. Spam puts a cost and a burden on recipients by clogging up network bandwidth, consuming disk space, and wasting employees' time. Spam is frequently a malware vector.

A "**Subscription service**" is a service whereby a software vendor offers software use and support for its product, usually for a predetermined period. For example: anti-virus vendors typically include a one-year subscription (for updates, notices, etc.) with the purchase of a product license. Many vendors offer fee-based subscription services whereby subscribers automatically receive updates, security bulletins, etc., for a set period.

A "**Target**" is the ultimate destination for malware; that which the malware is designed to attack. Boot sectors, hard disk drives, email servers, and departmental (HR, accounting, etc.) servers are examples of malware targets.

The "**Vector**" is how malware is carried to a computer, server, or system. An example would be an email attachment or embedded image.

IV. POLICY

A. MALWARE DEFENSE PLANNING

Malware is commonly passed to a potential target through email. The person who receives the email opens an attachment, which unleashes the malware, which then spreads to other computers via a shared network (malware may attack by other means, but this is a common method). To lessen the potential for damage to CCCE's Information Technology (IT) assets by malware, CCCE shall develop and implement a multifaceted approach to prevention.

To prepare CCCE's Malware Defense Plan, IT staff shall review the following items:

- Asset Inventory
- IT industry standards and best practices
- Anti-malware vendor websites or portals
- IT security alerts and bulletins (many of which are available for free and as a subscription service).

B. MALWARE DEFENSE PLAN

IT staff shall install/maintain firewalls on all workstations and servers.

IT staff shall ensure that operating systems, web browsers, email programs, and related software are configured for optimum security.

IT staff shall install an anti-virus program on every workstation and server and all anti-virus software shall be automatically updated using a subscription service (updates should be automatically logged by the software).

All anti-malware protections shall be configured to prevent being disabled by users. Only IT staff shall be allowed to temporarily disable anti-malware measures (for example, disabling a local antivirus program to install and configure an application).

CCCE shall minimize malware risks by backing up critical information.

C. MALWARE DEFENSE PLAN REVIEW

IT staff shall periodically review all anti-virus, firewall, and other relevant logs to determine if the software is up-to-date and is performing as expected.

D. MALWARE DEFENSE PLAN UPDATE

IT staff shall incorporate updates into the Malware Defense Plan as needed to address the latest trends in malware defense.

E. CONTAINMENT

Once a malware threat has been carefully analyzed it needs to be effectively contained so that the infection will not continue to spread. IT will develop a strategy to halt malware propagation. Once the strategy has been outlined the procedures to contain the malware threat should be followed quickly and efficiently. Procedures to contain the threat may include (but are not limited to):

- Power off infected systems
- Disable network access and isolate infected systems
- If the vector is from outside the network, disable network services
- Host, service, and application hardening

  Vulnerable systems should be protected by isolating network communication and applying service, application, and operating system updates as necessary

F. ERADICATION

After analysis and containment of a malware outbreak the threat needs to be removed from all infected hosts. Steps may include:

- Scan with installed antivirus software (make sure current definitions are installed)
- Clear system cache and temporary files
- Clear browser cache and temporary files
- Check browser add-ons or extensions
- Check recently installed applications or application updates
- Check browser settings for redirectors, start pages, or search engine changes
- Restore from backup media (use system restore, wipe drive, full format)
- Reload operating system (wipe system and load operating system)

G. RECOVERY

After the malware threat has been effectively eradicated from infected hosts the process of restoring the confidentiality, integrity, and availability of system software and data begins.

- Reinstall from backup or installation media
- Restore data from backup media
- Validate system state

  The host should have security software reinstalled and the application software should be tested to ensure that it functions properly.
- Restore network connectivity

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

IT staff will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. NON-COMPLIANCE

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.