COMMONWEALTH OF VIRGINIA

Department of General Services
Systems and Information Integrity Policy

Approved by: _____
Joe Damico - DGS Agency Head

Effective Date: 05/13/19

1 PURPOSE

The purpose of this policy is to create a prescriptive set of processes aligned with applicable COV IT security policies and standards, to ensure the Department of General Services (DGS) develops, disseminates, and updates the System and Information Integrity Policy. This policy establishes the minimum requirements for the System and Information Integrity Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.17 IT System and Information Integrity Family, controls SI-1 through SI-10 as well as additional Commonwealth of Virginia controls.

2 SCOPE

All DGS employees (classified, hourly, or business partners) as well as all DGS systems

3 ACRONYMS

COV:	Commonwealth of Virginia
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC501:	Information Security Standard 501
SSP:	System Security Plan
DGS:	Department of General Services

4 BACKGROUND

The System and Information Integrity Policy at DGS is intended to facilitate the effective implementation of the processes necessary meet the system and information integrity requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that DGS meet these requirements for all IT systems.

5 STATEMENT OF POLICY

In accordance with SEC501, SI-1 through SI-10, DGS shall develop, disseminate, and periodically review/update a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formalize documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

A. FLAW REMEDIATION

1. The System Owner shall identify, report, and correct information system flaws.

Note: Flaws include errors in software, as well as errors in configuration settings for information systems. Flaw remediation encompasses installing software patches, service packs, and hot fixes, as well as making changes to configuration settings. Vulnerability mitigation can also involve removing software or disabling functions, ports, protocols, and/or services.

2. An inventory of information systems and components must be collected and maintained by the System Owner in order to determine which hardware equipment, operating systems, and software applications are in operation.
    a. When flaw remediation and vulnerability mitigation activities are completed, the inventory of information systems and components must be updated to reflect current software versions and configurations.
    b. Refer to the DGS Configuration Management Policy for inventory requirements.
3. System Administrators shall test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation.
    a. All remediation changes must be tested on non-production systems prior to implementation on all IT products and configurations in order to reduce or eliminate the following:
        i. Unintended consequences
        ii. Alteration of security settings
        iii. Enabling of default user accounts that had been disabled
        iv. Resetting of default passwords for user accounts
        v. Enabling of services and functions that had been disabled
        vi. Non-security changes, such as new functionality
    b. Testing of patches must ensure that patches are installed in the required sequence and any removal of any previous security patch is not unintended.
    c. Testing must include checking all related software to ensure that it is operating correctly.
    d. Testing must include a selection of systems that accurately represent the configuration of the systems in deployment.
    e. Based on the results of testing, it must be considered whether any significant disadvantages outweigh the benefits of installing a patch and whether remediation should be delayed until the vendor releases a newer patch that corrects the major issues.
4. The ISO shall require that flaw remediation is incorporated into DGS's hardening process.

a. A patch and vulnerability list must be developed as part of the patch management lifecycle and must address the following:
    i. All equipment, operating systems, and software applications must be included.
    ii. The responsible party for monitoring and coordinating with each vendor for patch release support must be designated.
    iii. The responsible party for testing patches must be identified and coordinated.
    iv. Information security patches shall be installed in accordance with configuration management plans.
b. Vulnerability and flaw remediation actions must be tracked and verified.

5. Security sources for vulnerability announcements (i.e., both patch and non-patch remediation) and emerging threats that correspond to the software within the information system's inventory must be monitored by the System Owner.
    a. Information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) must be reported to designated organizational officials with information security responsibilities (e.g., Senior Information Security Officers, Information System Security Managers, Information Systems Security Officers).

    Note: Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems.

6. Security-relevant software updates (e.g., patches, service packs, and hot fixes) must be installed promptly by DGS and by contractors connecting to DGS systems.
    a. All software publisher security updates must be applied to the associated software products.
    b. All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.
    c. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.
7. The ISO or designee shall prohibit the use of software products that the software publisher has designated as End-of-Life/End-of-Support (i.e. software publisher no longer provides security patches for the software product).

a. Exceptions to End-of-Life/End-of-Support must be signed by the agency head and submitted to VITA CSRM for approval.

B. MALICIOUS CODE PROTECTION

1. The ISO or designee shall enforce the following requirements:
    a. Malicious code protection mechanisms must be employed at information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
        i. The following must be scanned:
            1. All inbound and outbound files.
            2. All email stored, inbound or outbound, including macros, with or without attachments, regardless of destination address.
            3. Email attachments prior to sending or opening.
            4. ActiveX and Java components in web pages and HTML-based email messages.
        ii. A content filtering package or additional device capable of blocking specified attachments must be installed and maintained on email servers.
            1. Attachments of the following types should be blocked: .ad, .ade, .adp, .ani, .asp, .bas, .bat, .bin, .ceo, .cfm, .chm, .cmd, .com, .cpl, .crt, .dll, .eml, .exe, .hlp, .htm, .html, .inf, .ins, .isp, .job, .js, .jse, .jsp, .lnk, .mde, .midi, .mov, .mp3, .mpeg, .msc, .msi, .msp, .mst, .net, .pcd, .php, .pif, .rar, .reg, .scr, .sct, .shb, .shs, .swf, .url, .vb, .vbe, .vbs, .vss, .vst, .vsw, .wmf, .ws, .wsc, .wsf, and .wsh.
        iii. Attachments and macros that cannot be scanned are deleted and replaced with a message detailing the action taken.
        iv. Outgoing email is scanned at the network server to which the client is connected.
    b. Standard malicious code protection software deployed on all workstations and servers must be configured to adhere to the following:
        i. Servers must be scanned for malicious code on a continuous basis.
        ii. Workstations must be automatically scanned for malicious code on a daily basis.

1. All forms of malicious code protection must start automatically upon system boot.
2. The boot sector and input devices must be scanned during system shutdown.

iii. Malicious code protection software must allow users to manually perform scans on their workstation and removable media.

iv. Malicious code protection software must be updated concurrently with releases of updates provided by the vendor of the software. Updates should be tested and/or approved according to DGS requirements.

c. Malicious code protection mechanisms must be used to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) that are:

i. Transported by electronic mail, electronic mail attachments, web accesses, removable media (e.g., Universal Serial Bus [USB] devices, diskettes or compact disks), or other common means.

1. If malicious code is detected in incoming or outgoing email (including attachments), the message and attachment are eliminated or quarantined as they attempt to enter or leave the email system.

ii. Inserted through the exploitation of information system vulnerabilities.

iii. Encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file.

d. Malicious code protection mechanisms (including signature definitions) must be updated whenever new releases are available and in accordance with agency-wide configuration management policy, procedures, and standards.

i. As applicable, the malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles.

ii. The information system must automatically update malicious code protection mechanisms (including signature definitions).

iii. The date of signature definitions must be monitored to ensure the automatic update is functioning properly.

e. Malicious code protection mechanisms must be configured to:

i. Perform periodic scans of the information system daily and real-time scans of files from external sources (e.g., network connections or input storage device) as the files are

downloaded, opened, or executed in accordance with DGS security policy.

ii. Block, clean, and/or quarantine malicious code and send alert to an administrator in response to malicious code detection.

iii. Automatically and periodically run scans on memory and storage devices.

iv. When feasible, scan all macros for malicious code.

v. Allow only authorized personnel to modify program settings.

vi. Maintain a log of protection activities, including, but not limited to, threat identification and response.

1. The logs are included in the backups.

2. Logs are maintained until no longer needed.

f. The following elements must be addressed during vendor and product selection and when tuning the malicious code protection software:

i. The receipt of false positives during malicious code detection and eradication.

ii. The resulting potential impact on the availability of the information.

Note: A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions and business functions.

g. In situations where traditional malicious code protection mechanisms are not capable of detecting malicious code in software (e.g., logic bombs, back doors), the organization must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

h. SSPs shall adopt a defense-in-depth strategy that integrates firewalls, screening, routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are consistently enforced.

i. Malicious code protection mechanisms must be centrally managed.
    i. Central management must include server-based solutions, not client-based.
        1. The server-based solution must automatically check and download new definition files and propagate the new files to all devices protected by the solution.

j. The information system must be configured to prevent non-privileged users from circumventing malicious code protection capabilities.
    i. End users must be prevented from disabling the protection on their computer.

2. The ISO or designee shall, or shall require that its service provider:
    a. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.).
    b. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.
    c. Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.
        i. Malicious code protection must be installed and maintained on all servers, workstations, laptops, and personal electronic devices regardless of operating system, whether connected to networks or not.
    d. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.
    e. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shutdown, restoration, notification, and reporting requirements.
    f. Require use of only new media (e.g. diskettes, CD-ROM) or sanitized media for making copies of software for distribution.
    g. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.
    h. By written policy, prohibit the installation of software on Agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.

i. Establish Operating System (OS) update schedules commensurate with sensitivity and risk.

j. Prohibit laptops from connecting to the network until authorized malicious code protection software is installed.

C. INFORMATION SYSTEM MONITORING

1. The ISO or designee shall enforce the following requirements:

   a. Events on the information systems must be monitored in accordance with defined monitoring objectives and information system attacks must be detected.

   Note: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network-monitoring software).

   b. Unauthorized use of the system must be identified.

   c. Monitoring devices must be strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17) to collect agency-determined essential information.

      i. These devices must be used to track the impact of security changes to the information system.

   Note: The Einstein network-monitoring device from the Department of Homeland Security is an example of a system monitoring device.

   Note: An example of a specific type of transaction of interest to the Agency with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required.

   d. The granularity of information collected must be determined based upon agency monitoring objectives and the capability of the information system to support such activities.

   e. The information system must be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions including, but not limited to:

      i. Internal traffic that indicates the presence of malicious code within an information system or propagating among system components

ii. The unauthorized export of information

iii. Attack signatures

iv. Signaling to an external information system

v. Localized, targeted, and network-wide events

f. Evidence of malicious code must be used to identify potentially compromised information systems or information system components.

g. The information system must be configured to provide a near real-time alert when indications of compromise or potential compromise occur from the following sources:

i. Audit records

ii. Input from malicious code protection mechanisms

iii. Intrusion detection and prevention mechanisms

iv. Boundary protection devices, such as firewalls, gateways, and routers

h. The information system must be configured to prevent users from circumventing intrusion detection and prevention capabilities.

i. A wireless intrusion detection system should be employed to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

j. An intrusion detection system must be employed if wireless communications traffic passes from wireless to wire-line networks.

D. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

1. The ISO or designee shall enforce the following requirements:

a. Information system security alerts, advisories, and directives must be received from designated external organizations on an ongoing basis;

i. All security alerts, advisories, and directives must be from reputable sources (i.e., VITA, vendors, and manufacturers).

b. Internal security alerts, advisories, and directives must be generated, as deemed necessary.

c. Security alerts, advisories, and directives must be disseminated to DGS personnel identified by name and/or by role.

d. Security directives must be implemented in accordance with established time frames, or the issuing organization must be notified of the degree of noncompliance.

E. SPAM PROTECTION

1. The ISO or designee shall enforce the following requirements:
    a. Spam protection mechanisms must be employed at information systems entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
    b. Spam protection mechanisms must be used to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.
    c. Spam protection mechanisms (including signature definitions) must be updated when new releases are available.

F. INFORMATION INPUT RESTRICTIONS

1. The ISO or designee shall require that the capability to input information to the information system is restricted to authorized personnel.
2. Note: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

G. INFORMATION INPUT VALIDATION

1. The ISO or designee shall enforce the following requirements:
    a. The information system must be configured to check the validity of information inputs.
        i. The checks for input validation must be verified as part of system testing.
    b. The information system must be configured to check all arguments or input data strings submitted by users, external processes, or untrusted internal processes.
        i. The information system must validate all values that originate externally to the application program itself, including arguments, environment variables, and information system parameters.
    c. Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) must be in place to verify that inputs match specified definitions for format and content.
    d. The information system must be configured to perform the following input validations:
        i. Type checks – Checks to ensure that the input is, in fact, a valid data string and not any other type of object.

1. This includes validating that input strings contain no inserted executable content or active content that can be mistakenly interpreted as instructions to the system, including, but not limited to: Trojan horses, malicious code, metacode, metadata, or metacharacters, Hypertext Markup Language (HTML), Extensible Markup Language (XML), JavaScript, Structured Query Language (SQL) statements, shell script, and streaming media.
2. Inputs passed to interpreters must be prescreened to prevent the content from being unintentionally interpreted as commands.

ii. Format and syntax checks – Checks to verify that data strings conform to defined formatting and syntax requirements for that type of input.

iii. Parameter and character validity checks – Checks to verify that any parameters or other characters entered, including format parameters for routines that have formatting capabilities, have recognized valid values.

1. Any parameters that have invalid values must be rejected and discarded.
2. Web server applications must be configured to prohibit invalid data from web clients in order to mitigate web application vulnerabilities including, but not limited to, buffer overflow, cross-site scripting, null byte attacks, SQL injection attacks, and HTTP header manipulation.

e. Invalid inputs or error statements must not give the user sensitive data, storage locations, database names, or information about the application or information system's architecture.

OTHER REFERENCE

ITRM Information Security Policy (SEC519)

ITRM Information Security Standard (SEC501)

Publication Revision Control

Version	Date	Purpose of Revision
Original	09/29/17	Base Document
2	01/29/18	New Agency Head
2.1	5/13/19	Updated references and title page