Information Technology Policy

Information Technology Security Assessment and Testing Policy

Number ITP-SEC023	**Effective Date** April 19, 2007
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** May 2024

1. Purpose

This Information Technology Policy (ITP) addresses the enterprise-wide need and provides guidance for Information Technology (IT) security Assessment and testing.

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITPs as outlined in the Responsibilities section.

3. Background

IT security Assessment and testing is a security practice designed to proactively identify, remediate, and prevent the exploitation of IT vulnerabilities that exist within an organization. During the process, IT related vulnerabilities are identified, and the risks of those vulnerabilities are evaluated. The evaluation leads to correcting the vulnerabilities and removing the risk or providing formal risk acceptance by the management of an organization. Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information.

Because vulnerabilities within any agency could potentially pose a threat to all agencies given shared network resources between all agencies, each agency shall assess all IT related risk Assessment reports and have a plan to mitigate and correct any risks deemed "critical or high". This policy minimizes the collective security risks associated with vulnerabilities to all agencies. Therefore, the Assessment and testing of security controls and processes are vital exercises for any organization.

4. Policy

The Office of Administration, Office for Information Technology (OA/IT), Enterprise Information Security Office (EISO) is responsible for conducting ongoing security Assessments on IT related systems and applications on the Commonwealth's enterprise network. These Assessments are used to benchmark the Commonwealth's IT security readiness and risk posture. As part of this process, vulnerability scans are regularly conducted on IT related systems. In addition, agencies will be asked to remediate pertinent vulnerabilities, complete questionnaires, conduct internal audits, and perform IT security tests to ensure that they are compliant with the Commonwealth's IT policies, procedures, and standards.

- Systems and services that interact with the public, or are on the Metropolitan Area Network (MAN) and not in a Demilitarized Zone (DMZ), whether it processes or stores sensitive or confidential information (as indicated in *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data* and *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information (PII)*) *or provides non classified information, shall undergo* Technical Security Reviews to ensure compliance with implementation standards and to ensure vulnerabilities to subsequently discovered threats are not present.

- Critical agency functions shall be maintained by each agency. Reviews of IT systems and services essential to supporting a critical agency function shall be conducted at least once every year. Reviews of a representative sample of all other systems and services shall be conducted at least once every two years.

- If an agency chooses to outsource the performance of security Assessments to an Independent Third Party, the Commonwealth Chief Information Security Officer (CISO) shall be notified, via email to ra-CISO@pa.gov, prior to finalizing the scope of the Assessment and offered the opportunity to request additional information regarding the selected Independent Third Party and the method of Assessment proposed.

- Agencies who are having audits conducted on a system, network, application, or service shall provide unauthenticated or authenticated host scans and Dynamic Application Security Testing (DAST) scans to Agency ISO for compliance review. If detailed reports are unavailable, a letter of attestation showing the compliance status shall be provided.

- Service Organizations shall ensure all solution components are securely coded, vetted, and scanned. To this end, the Service Organization will be required to provide host and application scan data to the Agency ISO whom the hosting services are being performed for. For propriety code or applications/software as a service (SaaS), a letter of attestation showing that the code is properly vetted, and applications are managed will suffice.

5. Assessment Testing and Remediation of Deficiencies

Agencies shall follow a three-step process for Assessment testing and remediation of deficiencies:

5.1 Assessment Tests

Assessment tests can be performed by agencies, the EISO, or a qualified Independent Third Party that is not currently implementing or managing the systems that will be reviewed.

Agencies can engage EISO to perform testing by using the Commonwealth ITSM tool Service Catalog. Additional costs may apply.

5.2 Mitigate and Remediate

Agencies are required to initiate mitigation of critical deficiencies within five (5) calendar days of the discovery of a critical deficiency. High level deficiencies shall initiate mitigation within ten (10) calendar days. Medium level deficiencies shall initiate mitigation within thirty (30) calendar days.

Agencies shall report on remediation of deficiencies discovered to the EISO at ra-CISO@pa.gov within thirty (30) calendar days of the discovery of a critical deficiency.

The following information is required in remediation reporting of critical deficiencies: (Agencies may use existing reports or formats that suit agency business needs.)

- Vulnerability Identifier (Name)
- CVE ID, CWE ID, and Vendor supplied ID number (if applicable)
- Scan Date (if applicable)
- Commonwealth ITP or MD in violation
- Application name and function
- Vulnerability Description
  - Mitigation Status (not started/initiated/completed)
  - Remediation Action (actions to be taken to remediate vulnerability)
- Estimated Remediation Completion Date

5.3 Retest

Upon completion of the remediation of a vulnerability, agencies shall retest for the existence of the remediated vulnerability. Agencies may perform the retest or request that the EISO perform a retest. Agencies can engage the EISO to perform a retest by using the Commonwealth ITSM tool.

The EISO is required to complete the retest and provide agencies with results within thirty (30) days of an agency request for a retest.

6. Network Vulnerability Scanning and Testing

The EISO monitors network activity to ensure that the Commonwealth's networks and systems are not compromised by internal and external threats and quickly remediated when they are. As part of this process, the Commonwealth's CISO may become aware of potential intrusions by unauthorized users. Scanning and testing for vulnerabilities can often produce attack signatures that can trigger automated control responses and generate notifications. Information Security teams need to differentiate between attack signatures that are expected and authorized as part of the scanning process from those that may have been generated by a real attack. To facilitate this awareness, all entities that are coordinating or conducting authorized scanning shall comply with the following:

A. Any host, network, or application vulnerability scanning shall be coordinated with the appropriate agency Information Security Officer (ISO) and the EISO. As part of this process, the agency ISO needs to contact the EISO to alert it of any potential testing that could set off a security alarm.

B. All agency-owned hosts shall be scanned for vulnerabilities and weaknesses before being installed on the network, and shall only be installed after the

resultant software, operating system, or configuration changes are made. For both internal and external systems, scans shall be performed monthly to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans is determined by the agency ISO and the information owner(s), depending on the criticality and sensitivity of the system's information along with any applicable regulatory requirements.

C. Network, host, and application vulnerability scanning shall be conducted after new software or major configuration changes are made on systems that are essential to supporting a process critical to an agency's mission. Scanning is conducted on all other systems on a monthly basis. The output of the scans shall be reviewed within 14 calendar days by the agency ISO and any vulnerability detected shall be evaluated for risk and false positive enumeration, and shall be mitigated or accepted as appropriate. The tools used to scan for vulnerabilities shall be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

D. Where an agency has outsourced a server, application, or any network service to another agency, external entity, or cloud service, both parties are responsible for coordinating any vulnerability scanning and ensuring the agency ISO is provided a monthly report. The output of the scans shall be reviewed within 14 calendar days by the agency ISO and any vulnerability detected shall be evaluated for risk, false positive enumeration and shall be mitigated or accepted, as appropriate. When an agency server or services are hosted by the Enterprise Data Center, the scanning shall be coordinated through the Commonwealth CISO.

E. Any authorized scanning shall follow a defined and tested process:

- **Test Plan:**
  Prior to conducting a Penetration Test, agency ISOs shall submit a test plan to the Commonwealth CISO. This test plan shall be submitted via email to: ra-CISO@pa.gov.

  Upon submission, the plan will be reviewed by the Commonwealth CISO to ensure the test will not interfere with Commonwealth business or damage Commonwealth information technology assets.

  NOTE: Failure to submit a test plan could trigger a false alarm in the Commonwealth's security monitoring, which could cause the agency to temporarily lose Internet access until the event can be investigated.

- **Scope:**
  The scope of what shall be examined needs to be explicitly named (systems, network ranges, applications, etc.). It is not permissible to extend the test beyond what was originally requested. Any vulnerability scan that extends beyond an agency will need to have the Commonwealth CISO and other agency ISOs formal approval documented. Any Penetration Test that goes beyond its authorized scope will be terminated. Items to be considered in a scope document can include:
  - Source networks where scans will originate from.
  - Tools that will be used.
  - Network ranges or web application URLs.
  - Types of scans to be performed, such as TCP, UDP, ports to be tests

and web application scans.

F. Results of scans that indicate vulnerabilities shall be shared with the agency ISO and other appropriate staff, including the EISO.

G. Agencies shall notify the EISO and the Commonwealth CISO before performing any external network scanning that was previously approved and coordinated with the Commonwealth CISO.

H. Users shall not test or attempt to compromise computer or network security measures at either the Commonwealth or other Internet sites, unless specifically authorized to do so. If users probe security mechanisms, alarms are triggered, and resources are needlessly spent tracking the activity. Unauthorized attempts to compromise security measures are unlawful and are considered serious violations of Commonwealth policy.

7. Agency Self-Assessment – Nationwide Cyber Security Review (NCSR)

The NCSR, or Nationwide Cyber Security Review, is a self-Assessment survey designed to evaluate cyber security management. The Federal Government has requested an ongoing effort to chart nationwide progress in cybersecurity and identify emerging areas of concern. In response, the U.S. Department of Homeland Security (DHS) has partnered with the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS- ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop and conduct the NCSR. The NCSR is designed to capture the nationwide level of cyber security preparedness and resilience within all State, Local, Territorial, and Tribal governments.

The NCSR establishes a uniform IT Security Assessment that will identify the Commonwealth's IT security readiness. This self-Assessment is based on a control security model identified as the NCSR Control Maturity Model. This model was created by the Software Engineering Institute (SEI) at Carnegie Mellon University. The NCSR provides the Commonwealth's IT departments with metrics that split IT security into categories. These categories are then assessed on a risk Assessment metrics that enables them to assess their IT security readiness.

Agencies shall ensure that they comply with the following policies and procedures:

7.1 Procedure

As part of the NCSR self-Assessment process, agencies will complete the Assessment on an annual basis. To ensure baseline reporting and metrics on individual and agency cyber preparedness, all agency primary ISO's (or equivalent) are required to participate in the NCSR. The NCSR shall be completed annually from October 1st to November 30th each year. Normally, the Assessment shall take the agency ISO one to several hours to complete and shall be completed with the assistance of whatever agency technical resources are necessary. To complete the survey, the agency ISO will be provided with the link to access the survey 2 weeks before the survey window is initiated. When completed, the Assessment is automatically saved by the application and an agency can view where it ranks in the given categories and how they compare to previous results over time.

When completing the NCSR self-Assessment, agencies will be asked to select a weighted response that best describes their current status for the given category. The agency will complete the process for all categories. All sections shall be

completed to ensure 100% completion of the survey.

7.2 Risk Assessment Metrics

The model uses an Assessment that has six levels that describes the agency's current readiness status. These levels are:

- Ad Hoc – Activities for this control are one or more of the following:
  - Not performed;
  - Performed but undocumented/unstructured; and/or
  - Performed and documented, but not approved by management.
- Documented Policy – The control is documented in a policy that has been approved by management.
- Documented Standards/Procedures – The control meets the requirements for Documented Policy and satisfies all of the following:
  - Documented standards and procedures to help guide implementation of the policy; and
  - Communicated to all relevant entities.
- Risk Measured – The control meets the requirements for Documented Standards/Procedures and satisfies all of the following:
  - Control is at least partially assessed to determine risk; and
  - Management is aware of the risks.
- Risk Treated - The control meets the requirements for Risk Measured and satisfies all of the following:
  - A risk Assessment has been conducted;
  - Management makes formal risk-based decisions based on the results of the risk Assessment to determine the need for the control; and
  - The control is deployed in those areas where justified by risk, but is not deployed where not justified by risk.
- Risk Validated – The control meets the requirements for Risk Treated and satisfies all of the following:
  - If the control is implemented in those areas where justified by risk, the effectiveness of the control has been externally audited/tested to validate that the control operates as intended; and
  - If the control is not implemented in those areas where not justified by risk, management's decision to not implement the control was determined to be sound.

7.3 Compliance

Annual enforcement is conducted. Agencies that do not complete the annual NCSR Assessment may be required to complete more extensive surveys and/or receive an onsite audit from the Commonwealth's CISO.

8. Penetration Testing/Ethical Hacking

A Penetration Test is a method of evaluating a computer system's or network's security by simulating an attack by a malicious entity. The intent of a Penetration Test is to determine feasibility of an attack and the toll a successful attack would have on the system, network, or application.

Penetration Tests are different than network Assessments because they often require the tester to use hacking and exploitation tools (e.g., Nmap, Metasploit, Core Impact, Cobalt Strike, Burp, Zap, Kali Linux, and other offensive style tools) to exploit known and unknown security vulnerabilities in hardware devices, networks, desktops, servers, and/or applications. In some instances, the use of these tools can damage the target that is being tested. Testers and their respective agencies need to be aware of the risks associated with Penetration Testing.

The typical Penetration Test involves an analysis of the system for potential vulnerabilities that may result from poor or improper system configuration, hardware or software flaws, or operational weaknesses in process or technical countermeasures. During the test, the tester will document:

- The process used in the analysis of the system;
- Any known and/or unknown hardware or software flaws;
- Operational weaknesses in process or technical countermeasures;
- Anticipated results (if known);
- Findings; and
- Recommendations to mitigate the risks discovered during testing.

When completed, testers will work with their operations teams, application developers, database administrators, and agency ISO to address any shortcomings discovered during the tests. The tester shall also meet with agency information technology leadership to discuss proper implementation and protection strategies.

8.1 Penetration Testing Strategies

- **Test Plan**
  Prior to conducting a Penetration Test, Agency ISOs shall submit a test plan to the Commonwealth CISO. This test plan shall be submitted via email to: ra-CISO@pa.gov.

  Upon submission, the plan will be reviewed by the Commonwealth CISO to ensure that the test will not interfere with Commonwealth business or damage Commonwealth information technology assets.

  Note: Failure to submit a test plan could trigger a false alarm in the Commonwealth's security monitoring, which could cause the agency to temporarily lose Internet access until the event can be investigated.

- **Scope**
  The scope of what shall be examined needs to be explicitly named (systems, network ranges, applications, etc.). It is not permissible to extend the test beyond what was originally requested. Any Penetration Test that extends beyond an agency will need to have the Commonwealth CISO and other agency ISOs formal approval documented. Any Penetration Test that goes beyond its authorized scope will be terminated. Items to be considered in a scope document can include:
  - Network ranges or web applications.
  - Types of attacks that are permitted or not permitted.
  - Denial of service potential.
  - Phishing/whaling/vishing scenarios.
  - Social Engineering.
  - Data exfiltration.
  - Use of malware or custom code.
  - Pivoting to other systems, networks, or applications.

- **Findings**
  After completing the Assessment or test, the agency ISO shall submit a synopsis of the findings to the Commonwealth CISO. The synopsis shall be submitted via email to ra-CISO@pa.gov with the original request and include the following:

  - Scope of the test, including assets, networks, and systems;
  - Description of methodology used;
  - Detailed results of the testing performed;
  - Indications of the results; and
  - Mitigation strategies that were implemented.

- **Agreements**
  Many aspects of a Penetration Test are intrusive and can damage the computer system or network. For the parties involved in the Penetration Test to fully understand the risks associated with it, the agency ISO needs to draft an agreement that identifies the risks and mitigation strategies associated with the Penetration Test process. This agreement shall be signed by all parties (agency and owners of host or networks being reviewed) involved in the test and shall clearly identify:

  - Type of Test.
  - Potential Risks:
    - Potential interruptions.
    - Potential loss or damage to data.
    - Potential loss or damage to equipment.
  - Mitigation Strategies.

  This document shall be submitted to the Commonwealth CISO and the EISO when notice is provided that a penetration test is being conducted.

- **Test Environment**
  Penetration Testing shall be conducted after hours and shall be conducted in a controlled environment. The only exception is when testing needs to be conducted in a production environment. In these instances, the agency ISO shall ensure that this is described in the test plan and agencies are urged to try to complete their tests during the maintenance window policy referenced in ITP-SYM010 - *Enterprise Services Maintenance Scheduling*.

- **System Archiving**
  Agency administrative personnel need to ensure that they archive system configurations and sensitive information before performing a Penetration Test. Penetration testers also need to show restraint regarding Commonwealth assets and data.

- **Freeware**
  The use of freeware penetration tools is permissible if they are approved by the Commonwealth CISO and they comply with *ITP-SFT001, Software Licensing* prior to being utilized.

9. Responsibilities

9.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

9.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

9.3 Third-party vendors, licensors, contractors, or suppliers shall:

Perform Assessments, audits, vulnerability scanning, and/or Penetration Testing consistent with the standards as outlined in this ITP.

10. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/Glossary.aspx*
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *ITP-SFT001, Software Licensing*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC024, IT Security Incident Reporting Policy*
- *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information (PII)*
- *ITP-SYM010, Enterprise Change Management Maintenance Policy*
- *MITRE's CWE ID Search*
- *MITRE's CVE ID Search*

11. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

12. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

13. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	4/19/2007	Base Policy	N/A
Revision	11/17/2011	Updated edits	N/A

Version	Date	Purpose of Revision	Redline Link
Revision	4/2/2014	Merged OPD-SEC023A, OPD-SEC023B, OPD-SEC023C, OPD-SEC023D into ITP	N/A

Revision	5/7/2015	• Expanded Purpose Section
		• Removal of Contingency and Continuity Planning section
		• Added Assessment Testing and Remediation of Deficiencies section
		• Updated Agency Self-Assessment section
		  ○ Removed biannual Assessments model
		  ○ Added annual Nationwide Cyber Security Review (NCSR) model
		• Removed ITP-APP001 reference in Section 7 Penetration Testing and Assessment – Freeware; replaced with ITP-APP033 Use of Freeware Policy
			N/A

Revision	04/27/2022	• Language added for third party vendors/responsibilities section updated. • Timelines added for review of vulnerabilities by Agency ISOs with action attached. • Policy links/references updated. • Definitions added for Assessment, CVE ID, CWE ID, Independent Third Party, Penetration Testing/Ethical Hacking, Technical Security Reviews, Vulnerability Assessment. • Test plan and scope added to Network Vulnerability Scanning and Testing. • Scope added to Penetration Testing/Findings updated. • Added 4th & 5th bullets under Policy to address audits and outsourced scans.	N/A
Revision	05/05/2023	• Expanded scope to include any entity connecting to the Commonwealth Network. • Definitions replaced with links to glossary. • Frequency of scans updated from quarterly to monthly. • Added remediation timeline for Assessments – high level deficiencies – 10 days, medium level deficiencies – 30 days. • Expanded criteria for systems and services which require technical security review.	Revised IT Policy Redline <05/05/2023>