pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Technical Security Assessments Policy

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

1. Purpose

This Information Technology Policy (ITP) provides guidance for Technical Security Assessments including, but not limited to, security tests, reviews, assessments, and audits. This policy minimizes the collective security risks associated with deficiencies in all agencies connected to the Commonwealth Network.

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 ITP as outlined in the Responsibilities section.

3. Definitions

Technical Security Assessments: A series of security tests, reviews, assessments, and audits conducted for discovering vulnerabilities in IT systems and services that may cause significant risk to an organization.

4. Policy

Technical Security Assessments shall be conducted on all systems and services that:

1. Interact with the public; or
2. Are on the Metropolitan Area Network (MAN) and not in a Demilitarized Zone (DMZ).

Technical Security Assessments shall be conducted when a system or service:

1. Processes or stores Class "C" or Closed Records (as indicated in *ITP-INF015, Policy and Procedures for Identify, Classifying, and Categorizing Commonwealth Electronic Data* and *ITP-SEC025, Proper Use and*

Disclosure of Personally Identifiable Information (PII)); or

2. Provides non-classified information (information that is not classified as Class “C” or Closed Records as above) to ensure compliance with implementation standards and that vulnerabilities from previously discovered threats are not present.

Agencies shall maintain a listing of critical agency functions. IT systems and services essential to supporting these critical agency functions shall have Technical Security Assessments conducted on them at least once (1) every year. Technical Security Assessments of a representative sample of all other systems and services shall be conducted at least once every two (2) years.

4.1 Roles & Responsibilities

The Office of Administration, Office for Information Technology (OA/IT) Enterprise Information Security Office (EISO) is responsible for conducting ongoing Technical Security Assessments on IT systems and services on the Commonwealth network. These assessments are used to benchmark the Commonwealth’s IT security readiness and risk posture. Agencies may choose to outsource the performance of the Technical Security Assessments to an Independent Third Party.

Agencies that choose to outsource the Technical Security Assessments shall ensure notification is provided to the OA as outlined in the appropriate supporting policy document no less than 5 business days prior to the start of the assessment. This is to provide the opportunity for the OA to request additional information regarding the selected Independent Third-Party and the method proposed.

Service Organizations shall ensure all solution components are securely coded, vetted, and scanned. To this end, the Service Organization will be required to provide scan data from the required Technical Security Assessments to the Agency Information Security Officer (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. Agencies and Services Organizations shall ensure all work performed is in alignment with *ITP-SEC000, Information Security Policy*, section 4.1 Offshore Access.

Agencies that are having assessments conducted on systems and services shall provide reports to the Agency ISO and EISO Vulnerability Management Team (RA-OAEISOVulnMgmt@pa.gov) for a compliance review. If detailed reports are unavailable, a letter of attestation showing the compliance status shall be provided.

Agencies shall 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.

Agencies shall read and comply with the following supporting policy documents *(Commonwealth access only),* which will provide detailed information about the required Technical Security Assessments:

1. *OPD-SEC023A, Security & Compliance Assessment Testing*
2. *OPD-SEC023B, Network Vulnerability Scanning*
3. *OPD-SEC023C, Penetration Testing*
4. *OPD-SEC023D, Nationwide Cyber Security Review*

5. Responsibilities

5.1 Agencies shall:

Comply with the requirements as outlined in this ITP. This includes ensuring all Technical Security Assessments are conducted as required in supporting documents (OPD-SEC023A, OPD-SEC023B, OPD-SEC023C, OPD-SEC023D – *Commonwealth access only*).

5.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP. This includes conducting ongoing Technical Security Assessments on IT systems and services on the Commonwealth network as outlined in this ITP and supporting documents.

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

Perform assessments, audits, vulnerability scanning, and/or penetration testing consistent with the requirements as outlined in this ITP and supporting documents.

6. 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
- *OPD-SEC023A, Security & Compliance Assessment Testing (Commonwealth access only)*
- *OPD-SEC023B, Network Vulnerability Scanning (Commonwealth access only)*
- *OPD-SEC023C, Penetration Testing (Commonwealth access only)*
- *OPD-SEC023D, Nationwide Cyber Security Review (Commonwealth access only)*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC041, Commonwealth IT Resources Patching Policy*
- *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-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *ITP-SFT001, Software Licensing*
- *ITP-SYM010, Enterprise Change Management Maintenance Policy*
- MITRE’s CWE ID Search
- MITRE’s CVE ID Search

- Commonwealth ITSM

7. Authority

Executive Order, 2016-06 Enterprise Information Technology Governance

8. 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.

9. 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 Commonwealth 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
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

Version	Date	Purpose of Revision	Redline Link
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.	N/A
Revision	09/25/2023	• Title updated from "Information Technology Security Assessment & Testing Policy" to "Technical Security Assessments Policy" to better align with policy content. • Overall policy content separated placed into supporting documents based upon subject matter: ○ ITP is overall policy requirement on Technical Security Assessments (definition updated). ○ OPD-SEC023A policy on requirements/guidance on Security & Compliance Assessment Testing. ○ OPD-SEC023B policy on requirements/guidance on Systems & Services Vulnerability Scanning. ○ OPD-SEC023C policy on requirements/guidance on Penetration testing. ○ OPD-SEC023D policy on requirements/guidance on Nationwide Cyber Security Review (NCSR). • Purpose has been updated to reflect changes to ITP-SEC023. • Definition of Technical Security Assessments updated. • Use of "Technical Security Reviews" and "Reviews" updated to "Technical Security Assessments" and "Assessments" throughout policy. • Updated policy reference of ITP-SEC019 to ITP-INF015 in policy language and Related ITPs/Other References which provides guidance on classification of data. • Added references to new supporting documentation throughout policy and under Related ITPs/Other References. • Updated notification guidance for Technical Security Assessments. • Responsibilities section updated in alignment with policy modifications. • Reference added to ITP-SEC000 in relation to work within CONUS.	Revised IT Policy Redline <09/25/2023>