pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Information Technology Security Assessment and Testing Policy

ITP Number ITP-SEC023	***Effective Date*** April 19, 2007
Category Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

This Information Technology Policy (ITP) establishes enterprise-wide policy for information technology security assessment and testing.

1. Purpose

The assessment and testing of security controls and processes are vital exercises for any organization. Testing verifies the proper configuration of systems, the accuracy of documentation, and the skills of staff members. Assessments help determine gaps between an organization's current practices and its desired practices. To be effective, the testing of security controls is to be done in an organized and authorized manner. This Information Technology Policy (ITP) describes the policies surrounding security assessments and testing.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Policy

The Office of Administration/Office for Information Technology (OA/OIT) Information Security Office is responsible for conducting ongoing security assessments that are used to benchmark the commonwealth's Information Technology (IT) security readiness. As part of this process, agencies will be asked to 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. In addition to this, agencies are to ensure that they adhere to the following policies and procedures:

- Agencies are to read and comply with the following sections of this ITP, which will provide the agencies with detailed information about assessments, audits, and tests:

4. Network Vulnerability Scanning and Testing
5. Contingency and Continuity Planning
6. Agency Self-Assessment – IT Maturity Model
7. Penetration Testing and Assessment

- Systems and services that process or store sensitive or confidential information (as indicated in ITP-SEC019 and ITP-SEC025) or which provide support for critical processes are

to undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats.

- Critical agency functions are to be maintained by each agency. Reviews of systems and services that are essential to supporting a critical agency function are to be conducted at least once every year. Reviews of a representative sample of all other systems and services are to be conducted at least once every twenty-four months.

- If an agency chooses to outsource the performance of security assessments, the Commonwealth CISO is to be notified via email to RA-CISO@pa.gov prior to finalizing the scope of the assessment in order to ensure the assessment meets industry standard best practices.

- Remediation of deficiencies or recommendations that result from any assessment or testing is to be completed and reported to the Commonwealth Chief Information Security Officer (CISO) with the following schedule:

1) Action to remediate critical severity deficiencies/recommendations must be initiated immediately upon receipt of assessment/testing results; (after appropriate testing.

2) Remediation of high severity deficiencies/recommendations must be completed within 30 days upon receipt of assessment/testing results;

3) Remediation of remaining deficiencies recommendations must be complete within 90 days of receipt of assessment/testing results;

4) A corrective action report and impact analysis including expected date of remediation must be created within 30 days of receipt of assessment/testing results;

- Any deviations from expected or required results detected by the technical security review process are to be reported to the agency Information Security Officer (ISO) and a remediation process started immediately. In addition, the agency application/data owner is to be advised of the deviations and is to initiate investigation of the deviations (including the review of system activity log records if necessary).

4. Network Vulnerability Scanning and Testing

The Office of Administration/Office for Information Technology (OA/OIT) Information Security Office monitors network activity to ensure that the commonwealth's networks and systems are not compromised by internal and external threats. As part of this process, the office alerts the Commonwealth Chief Information Officer (CISO) of potential intrusions by unauthorized personnel. Sometimes these intrusions are real attacks and sometimes they are false positives created by agency security teams who are proactively monitoring their networks. In order to avoid potential false positives, the OA/OIT Information Security Office is asking agencies to comply with this supporting documentation.

This section addresses how network vulnerability scanning will be conducted in order to avoid potential false positives and to prevent possible attacks from internal and external threats. As part of this process, agencies are to comply with the following policies and procedures.

Any host or network vulnerability scanning or penetration testing is to be coordinated with the appropriate agency Information Security Officer (ISO). As part of this process, the ISO needs to contact the OA/OIT Information Security Office to alert it of any potential testing that could set off a security alarm.

- All agency-owned hosts that are or will be accessible from outside the agency's network are to be scanned for vulnerabilities and weaknesses before being installed on the network, and are only installed after the resultant software, operating system or configuration changes are made. For both internal and external systems, scans are to be performed annually 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.

- Network vulnerability scanning is to be conducted after new network 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 an annual basis. The output of the scans is to be reviewed in a timely manner by the agency ISO and any vulnerability detected is to be evaluated for risk and mitigated as appropriate. The tools used to scan for vulnerabilities are to be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

- Where an agency has outsourced a server, application or any network service to another agency or entity, both parties are responsible for coordinating any vulnerability scanning. When an agency server or services is hosted by the Enterprise Server Farm, the scanning is to be coordinated through the Enterprise Security Team (EST) and the Commonwealth CISO.

- Any authorized scanning is to follow a defined and tested process in order to minimize the possibility of disruption.

- Results of vulnerability scans that indicate susceptibilities are to be shared with the ISO and other appropriate staff.

- Agencies are to notify the Commonwealth's Chief Information Security Officer (CISO) and the EST before performing any external network planning that was previously approved and coordinated with the CISO and EST.

- Users are not to 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.

5. Contingency and Continuity Planning

The scope of section is limited to agency information technology (IT) infrastructures, data, and applications. Agencies are to adhere to the following guidelines to be compliant with this policy:

- As part of the contingency and continuity planning process, agencies are to conduct a threat and risk assessment to determine the criticality of business systems, and the time frame required for recovery. These assessments are to be done anytime the agency updates its contingency and continuity plans.

- Each agency business unit, including agency security management, in cooperation with the agency Chief Information Officer, is to develop plans that meet the IT backup and

recovery requirements of the agency. This is to ensure that interruptions to normal agency business operations are minimized, and agency business applications and processes are protected from the effects of major failures.

6. Agency Self-Assessment – IT Maturity Model

The intent of this supporting documentation establishes a uniform Information Technology (IT) security assessment that will identify the commonwealth's IT security readiness. This assessment is based on a security model identified as the IT Maturity Model. This model was created by the Software Engineering Institute (SEI) at Carnegie Mellon University.

The IT Maturity Model provides the commonwealth's IT departments with metrics that breaks IT security into twelve categories. These categories are then assessed on a risk assessment metrics that enables them to assess their IT security readiness.

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

Biannual Assessments

As part of the IT Maturity Model assessment process, agencies will have to complete the assessment on a biannual basis. These assessments are to start on the first week in July and January and each agency will be given one month to complete the assessments. After completing the assessment, the agency is to benchmark any deficiencies and initiate a plan to address them.

Information Security Officer (ISO)

The agency ISO will be responsible for completing the biannual assessment and work with Office of Administration/Office for Information Technology (OA/OIT) Chief Information Security Officer (CISO) to address any deficiencies. For more information on the duties and responsibilities of the ISO, please reference ITP-SEC016 - *Commonwealth of Pennsylvania – Information Security Officer Policy.*

Compliance

Agencies that do not complete the biannual assessment or that consistently rank "Level 2" or below (see section *Risk Assessment Metrics*) may be required to complete more extensive surveys and/or receive an onsite audit from the OA/OIT CISO.

Procedure

The IT Maturity Model is to be completed biannually by July 31 and January 31. Normally, the assessment is to take the ISO one business week to complete and is to be completed with the assistance of whatever agency technical resources are necessary (e.g., Project Management, Security, Operations, Applications, and Business Groups).

In order to complete the survey, the ISO is to access the Commonwealth's Cyber Security page located at: http://cybersecurity.state.pa.us and select "Commonwealth Employees" link.

The ISO is to use his or her Commonwealth of Pennsylvania Active Directory forest (CWOPA) identification and password to logon to the secured "Agency Assessment" link. After the IT Maturity Model opens, the ISO is to complete the assessment. The following describes the categories and risk assessment metrics.

Security Categories

Note: When completing the assessment, the agencies will be asked to select a weighted response that best describes their current status for the given category. The agency will repeat this process for all twelve categories. For more information on the metrics, refer to

the *Risk Assessment Metrics* section.

The following identifies the twelve security categories and how they are used to create the benchmarks:

1. Risk Assessment and Management – Measures the agency's current risk assessment and mitigation processes. The category also measures if an agency proactively addresses potential security risks.

2. Security Policy – Assesses the agency's current security policies and procedures to determine if they are in compliance with the Commonwealth's IT policies, procedures, and standards.

3. Organization of Information Security – Measures an agency's commitment to IT security. As part of the assessment, the agency needs to determine if it has staff and funding allocated to IT security. The agency is to also benchmark its commitment to conduct security assessments, and to address shortcomings with IT security policies, procedures, and standards.

4. Asset Management – Measures the agency's commitment to track its IT resources (Personal Computers, Laptops, Servers, BlackBerries, and storage tapes).

5. Human Resources Security – Measures an agency's commitment to track employee and contractor hiring, transfers, and separation activities as they relate to IT security. The areas that are evaluated include: activating and deactivating: user accounts, administrative accounts, and building access; security cameras; and access logs review.

6. Physical and Environmental Security – Measures an agency's commitment to ensure that its IT resources are safeguarded against potential threats from personnel, fires, and disasters. The areas that are evaluated include physical security policies and procedures, access logs, security devices, and fire retardants.

7. Communications and Operations Management – Measures an agency's commitment to ensure that agencies have policies and procedures to manage their information processing facilities. This includes validating that an agency has policies and procedures that:

   - Govern the management of the agency's information processing facilities.
   - Assign responsibilities for the day-to-day operations of the agency's information processing facilities.
   - Take into consideration capacity planning.
   - Address malicious code.
   - Address data loss.
   - Address information exchanges with outside agencies and business partners.
   - Monitor security events.

8. Access Control – Measures an agency's commitment to evaluate its access requirements to its data. This evaluation is to be based on laws, policies, and procedures. This policy also addresses the agency's commitment on properly applying or removing access for users, administrators, and developers.

9. Incident Management – Measures the agency's commitment to ensure that it has policies and processes in place to report, detect, and/or investigate security incidents in compliance with ITP-SEC024 - *IT Security Incident Reporting Policy.*

10. Business Continuity Management – Measures the agency's commitment concerning continuity recovery readiness and if the agency's plans take into consideration IT security as part of the planning process.

11. Compliance – Measures the agency's commitment to review its internal policies and procedures to ensure that access to its IT resources comply with existing legislation, regulations, policies, procedures, and product licenses.

12. Information Systems Application Development and Maintenance (AD&M) – Measures an agency's commitment to ensure that IT security is a part of its systems development process. This includes systems development, project development, or systems acquisition.

Risk Assessment Metrics

The model uses an assessment that has six levels that describes the agency's current readiness status for each of the twelve categories. These levels are:

- Level 0: Non-Existent – The need for IT security in the given category is not recognized.

- Level 1: Initial/Ad Hoc – The risks and events are addressed as needed but there are no defined policies or processes.

- Level 2: Repeatable but Intuitive – There is an emerging understanding of the importance of IT security but there are only fragmented policies and procedures.

- Level 3: Defined Process – IT security policies and procedures exist and they are supported by management and there are responsibilities assigned to agency staff.

- Level 4: Managed and Measurable - There are IT security policies and procedures that are followed and the agency consistently performs impact analysis and uses metrics to track its performance.

- Level 5: Optimized - There are IT security policies and procedures that are structured, implemented agency-wide, well-managed, and enforced. In addition to this, the agency consistently completes and implements findings from its impact analysis and metrics.

When completed, the assessment is automatically scored by the IT Maturity Model and an agency can see where it ranks in the given categories. Agencies that score a "Level 2" or below may be asked to complete more extensive assessments or undergo an onsite audit by the OA/OIT Security Team.

Note: Agencies that do not complete the assessment will automatically be given an assessment score of "Level 0" for that given period.

7. Penetration Testing and Assessment

A penetration test is a method of evaluating a computer system's or network's security by simulating a malicious attack by a virus, hacker, or cracker. The intent of a penetration test is to determine feasibility of an attack and the toll a successful attack would have on the system or network.

Penetration tests are different than network assessments because they often require the tester to use hacking and cracking tools (e.g., Nmap, Nessus) to exploit known and unknown security vulnerabilities in hardware devices, networks, and/or applications. In some

instances, the use of these tools can damage the target that 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.
- Recommendations to mitigate the risks discovered during testing.

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

Penetration Testing Strategies

- **Test Plan**
  Prior to conducting a penetration test, Agency Information Security Officers (ISOs) are to submit a test plan to the Commonwealth Chief Information Security Officer (CISO). This test plan is to be submitted online at: ra-ciso@state.pa.us

  Upon submission, the plan will be reviewed by the 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.

- **Findings**
  After completing the assessment/test, the ISO is to submit a synopsis of the findings to the CISO. The synopsis is submitted online with the original request and includes:

  - Detailed results of the testing performed.

  - Indications of the results.

  - Mitigation strategies that were implemented.

- **Agreements**
  Many aspects of a penetration test are intrusive and can damage the computer system or network. In order for the parties involved in the

penetration test to fully understand the risks associated with it, the ISO needs to draft an agreement that identifies the risks and mitigation strategies associated with the penetration test process. This agreement is to be signed by the parties involved in the test and is to clearly identify:

- Type of Test
- Potential Risks
  - Potential interruptions
  - Potential loss or damage to data
  - Potential loss or damage to equipment

- Mitigation Strategies

- **Test Environment**
  Penetration testing is to be conducted in a controlled environment. The only exception is when testing needs to be conducted in a production environment. In these instances, the ISO is to 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**
  Testers need to ensure that they archive system configurations and sensitive information before performing a penetration test. Testers also need to archive critical assets that may be jeopardized during the penetration test.

- **Freeware**
  The use of freeware penetration tools is permissible as long as they are approved by the CISO and that they comply with ITP-APP001 – *Commonwealth Software Policy* prior to being utilized.

8. Responsibilities

Agencies are required to perform the actions outlined in this policy.

9. References

- 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 Services Maintenance Scheduling*
- ITP-APP001 – *Commonwealth Software Policy*

10. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

11. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	4/19/2007	Base Policy
Revision	11/17/2011	Updated edits
	4/2/2014	ITP Refresh; Merged OPD-SEC023A, OPD-SEC023B, OPD-SEC023C, OPD-SEC023D into ITP