pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Information Technology Security Assessment and Testing Policy

ITP Number	***Effective Date***
ITP-SEC023	April 19, 2007
Category	***Supersedes***
Security	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	May 2016

1. Purpose

This policy addresses the enterprise-wide need for IT security assessment and testing. 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 must assess all IT related risk assessment reports and have a plan to mitigate and correct any risks deemed "critical". This policy when adhered to by all agencies minimizes the collective security risk associated with vulnerabilities to all agencies. Therefore, the assessment and testing of security controls and processes are vital exercises for any organization. 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) 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 Information Technology (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 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 to ensure vulnerabilities to subsequently discovered threats are not present.

• Critical agency functions are to be maintained by each agency. Reviews of IT systems and services 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 to a third party, 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 commonwealth guidelines and industry best practices.

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

4. **Assessment Testing and Remediation of Deficiencies**
5. **Network Vulnerability Scanning and Testing**
6. **Agency Self-Assessment – Nationwide Cyber Security Review (NCSR)**
7. **Penetration Testing and Assessment**

4. Assessment Testing and Remediation of Deficiencies

Agencies are to follow a three step process for assessment testing and remediation of deficiencies:

4.1. Assessment Test

Assessment tests can be performed by agencies or the Enterprise Information Security Office (EISO). Agencies can engage EISO to perform testing by using the Service Engagement Review Process (SERP).

4.2. Mitigate and Remediate

Agencies are required to initiate mitigation of critical deficiencies within five (5) calendar days of the discovery of a critical deficiency.

Agencies are to report on remediation of critical deficiencies to the EISO at ra-CISO@pa.gov within thirty (30) calendar day 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.)

- Scan Identifier (Name)
- Scan Date
- Application
- Vulnerability Description
- Mitigation Status (not started/initiated/completed)
- Remediation Action (actions to be taken to remediate vulnerability)
- Estimated Remediation Completion Date

4.3. Retest

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

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

5. Network Vulnerability Scanning and Testing

The Office of Administration/Office for Information Technology (OA/OIT) Enterprise Information Security Office (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 Chief Information Officer (CISO) may become aware 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 and to prevent possible attacks from internal and external threats, agencies are to comply with the following policies and procedures.

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

B. 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.

C. 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.

D. 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 Data Center, the scanning is to be coordinated through the Commonwealth CISO.

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

F. Results of scans that indicate vulnerabilities are to be shared with the agency ISO and other appropriate staff.

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

H. 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.

6. 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 Information Technology (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 breaks IT security into 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:

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 Nationwide Cyber Security Review (NCSR). The NCSR is to be completed annually from October 1st to November 30th each year. Normally, the assessment is to take the ISO one to several hours 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 will be provided 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 must be completed to ensure 100% completion of the survey.

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
  - 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
  - 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
  - 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
  - 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
  - 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

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.

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 to: ra-CISO@pa.gov.

  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 agency 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 shall be conducted after hours and 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 agency 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-APP033 – *Use of Freeware Policy* prior to being utilized.

8. Responsibilities

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

9. References

- ITP-APP033 – *Use of Freeware 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-SYM010 - *Enterprise Services Maintenance Scheduling*
- Service Engagement Review Process (SERP) - https://www.sp.state.pa.us/

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
Revision	4/2/2014	Merged OPD-SEC023A, OPD-SEC023B, OPD-SEC023C, OPD-SEC023D into ITP

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
		  o Removed biannual Assessments model
		  o 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