pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth Application Certification and Accreditation

ITP Number ITP-SEC005	***Effective Date*** April 30, 2009
Category Recommended Policy	***Supersedes***
Contact ra-oaitb@pa.gov	***Scheduled Review*** June 2022

1. Purpose

This Information Technology Policy (ITP) establishes policy, technical guidance, and security procedures relating to using, sending, receiving, and storing electronic records and electronic signatures in compliance with Act No. 69 of 1999 (73 P.S. § 2260.101, *et seq.*), known as the Electronic Transactions Act (Act) and Management Directive (MD) 210.12 *Electronic Commerce Initiatives and Security.*

This policy documents compliance with Chapter 5 of the Act. Chapter 5 of the Act, relating to governmental agencies, sets forth the rules for the acceptance and use of electronic transactions by governmental agencies. Chapter 5 of the Act also directs all executive agencies to comply with standards established by the Office of Administration (OA), the agency responsible for creating IT policies, procedures, and standards that promote consistency and interoperability between governmental agencies.

In addition, MD 210.12 *Electronic Commerce Initiatives and Security* requires agencies to complete a security assessment prior to participating in or initiating an electronic transaction involving the use, transmission, or storage of electronic records or electronic signatures. This assessment, the Commonwealth Application Certification and Accreditation $(CA)^2$ process, is the subject of this ITP.

The $(CA)^2$ process is an assessment tool that measures a proposed E- Government initiative's compliance with OA/Office for Information Technology (OA/OIT) IT policies, procedures, and standards. The $(CA)^2$ process also identifies the inherent risks associated with an existing or proposed E-Government initiative. The $(CA)^2$ process is authorization to operate from OA/OIT to agency owned websites.

2. Scope

This ITP applies to all departments, boards, offices, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of

this ITP that are applicable to the products and services provided to the Commonwealth.

This ITP sets forth the policies and procedures that agencies and OA/OIT/Enterprise Information Security Office (OA/OIT/EISO) are to adhere to when assessing Internet Facing Web Applications for potential vulnerabilities. For the purpose of this ITP, an Internet Facing Web Application is defined as an application that uses the Internet to provide citizens, Commonwealth employees, and business partners with access to agency-specific data or services that resides on Commonwealth IT resources.

Examples of Web applications include forms, login pages, dynamic content, and discussion boards.

OA/OIT/EISO must complete $(CA)^2$ assessments on:

- Internet Facing Web Applications hosted on the Commonwealth's network(s).
- Web application frameworks that have not been vetted through the $(CA)^2$ process. For more information about a Web application framework's accreditation status, please contact OA/OIT Service and Solutions to see if the framework has been accredited.
- Internet, Intranet, Extranet Web applications or Web application frameworks that process "Breach Act Data," "Sensitive Security Information," or may pose risk to the Commonwealth's IT infrastructure.
- Hardware and virtual devices that host Web applications, Web services, databases, etc.

This policy shall not apply to vendor hosted Web applications as long as the following conditions are met:

- The Web application and its components are hosted by the vendor. This includes components that support the application such as Web services, databases, etc.
- The terms and conditions of the contract place the responsibility for network and application security on the vendor. This includes host scanning, network vulnerability testing, Web application vulnerability scanning, PCI scanning, etc.
- The terms and conditions of the contract include a confidential information clause, Non-Disclosure Agreement or similar language that protects the Commonwealth's data.

3. Objective

To establish policy for the Commonwealth Application Certification and Accreditation $(CA)^2$ process.

4. Definitions

4.1 Internet Facing Web Application - is an application that uses the Internet to provide citizens, Commonwealth employees, and business partners with access to agency-specific

data or services and that resides on Commonwealth IT resources. This includes content generated from a data visualization or business analytics platform.

5. Policy

Agencies that have Web applications shall submit $(CA)^2$ requests to OA/OIT for accreditation review. This review consists of policy compliance assessments and vulnerability assessments, which include source code analysis, host-based intrusion scans, and Web application vulnerability assessments.

All Web applications that go through the accreditation process and have risks that cannot be remediated will be deemed as an "at risk application". System Owners shall provide a risk analysis, including probability and impact, and risk mitigation plan. The risk mitigation plan must identify and provide analysis of the risks associated with the Web application, planned mitigations and timeline, as well as identify how the agency plans to mitigate risk responses. This plan must be attached to the $(CA)^2$ submission and reviewed by the OA/OIT/EISO to determine if the application can go into production with a conditional accreditation.

In addition to new applications, accredited Web applications must undergo a reaccreditation process every three (3) years in order to maintain security accreditation and any changes to an accredited application's security architecture will void its accreditation status. In order to regain $(CA)^2$ accreditation, agencies shall submit a new or updated $(CA)^2$ request.

In addition to the security requirements established by the OA/OIT ITPs, there may also be agency-specific security requirements that are not captured by OA/OIT policy, procedures, and standards, such as federal or state laws or regulations, executive orders, or management directives.

Since these requirements are agency- or business-owner specific, it is the responsibility of the agencies to ensure:

- All required security controls mandated by law, agency policy, or business owner requirements are incorporated into the agency's Web application security architecture.
- All appropriate security requirements are addressed in agency acquisitions of information systems and information system services.
- All financial applications that use credit cards are compliant with Payment Card Industry Data Security Standards (PCI-DSS).

Non-accredited applications and conditionally approved applications will be deemed as an "at risk application." For the purpose of this policy, an "at risk application" is an application that:

- Is in production but has not undergone/completed the $(CA)^2$ assessment process.
- Has initiated the $(CA)^2$ process but receives a conditional approval due to business constraints or vulnerabilities that cannot be remediated at the time the

application needed to be put into production.

Applications that have started the $(CA)^2$ process but have not been updated within one year of the initial submission date will be automatically withdrawn in the $(CA)^2$ system, and the Application Inventory updated. This is being done to remove applications that are not ready to begin the assessment process, have been placed on hold, or have been cancelled and were not removed from the system.

Note: Submitters can avoid having applications removed from the $(CA)^2$ system by going into the system and submitting an update/status report in the system's comments field or by contacting the $(CA)^2$ Administrator.

6. Responsibilities

6.1 OA/OIT Chief Technology Officer (CTO) – The CTO reports to the Deputy Secretary for Information Technology and is responsible for the day-to-day operations of Commonwealth's IT infrastructure. As part of these duties, the CTO is to ensure that all Web applications being placed onto Commonwealth networks are secure and that potential vulnerabilities are either remediated or that a risk mitigation plan is in place before allowing Web applications to be put into production. In order to do this, the CTO will assist the Commonwealth Information Security Officer (CISO) to complete the $(CA)^2$ process on Web applications being hosted on Commonwealth networks.

6.2 CISO – The CISO reports to the Deputy Secretary for Information Technology and is responsible for protecting the Commonwealth's IT infrastructure from internal and external cyber security threats. This responsibility includes managing the OA/OIT/EISO which is responsible for completing the $(CA)^2$ process on existing and prospective Web applications.

In addition to managing the OA/OIT/EISO, the CISO will be responsible for putting together a board of technical experts and security advisors who will review $(CA)^2$ requests to determine if they present security threats to the Commonwealth's IT infrastructure. This board will be comprised of:

- **$(CA)^2$ Administrator** – The $(CA)^2$ Administrator is responsible for the administration of the $(CA)^2$ process. In addition to this, the $(CA)^2$ Administrator is responsible for:

    - Day-to-Day Operations – The $(CA)^2$ Administrator is responsible for addressing agency questions, comments or concerns, troubleshooting issues, and updating the $(CA)^2$ system to address changes in OA/OIT ITPs or security threats.

    - $(CA)^2$ System Administration – $(CA)^2$ Administrator will ensure the entry of and update user accounts in the $(CA)^2$ system.

    - $(CA)^2$ Review Board - The $(CA)^2$ Administrator will act as the $(CA)^2$ Review Board coordinator and schedule meetings between the $(CA)^2$ Review Board, $(CA)^2$ Points of Contact (POC), and agency personnel.

- **(CA)^2 Reviewers** – The CISO will be responsible for working with OA/OIT Bureau Directors to appoint representatives from their respective bureaus to participate on the (CA)^2 Review Board. The (CA)^2 reviewers will assist OA/OIT/EISO in evaluating (CA)^2 submissions and represent OA/OIT in instances where clarification is needed, or agencies request technical assistance.

- **(CA)^2 POC** – Agencies are responsible for appointing representatives, (CA)^2 POC, to act as the liaison between the agency, OA/OIT/EISO, and the (CA)^2 Review Board. In addition to this, (CA)^2 POC is responsible for:

  - Submitting Web Applications – The (CA)^2 POC is responsible for entering agency Web application information into the (CA)^2 system.

  - Updating Web Application Information – If there are changes to an application's security architecture, the (CA)^2 POC will be responsible for resubmitting the application through the (CA)^2 process. Changes to an application's security architecture that are not documented in the (CA)^2 system will cause the application to become non-accredited.

  - Triennial Reaccreditation – The (CA)^2 POC is responsible for ensuring that all Web applications due to be reaccredited are resubmitted through the (CA)^2 process before the application's expiration date.

Note: Failure to submit an application before the expiration date will cause the application to become unaccredited and the agency will assume the risk of allowing the application to continue to operate in this condition.

  - Contacting the OA/OIT/EISO – The (CA)^2 POC will be responsible for contacting the OA/OIT/EISO to add/delete (CA)^2 users, request assistance with security scans, and to request meeting with the (CA)^2 Review Board.

6.3 OA/OIT/EISO - OA/OIT/EISO is headed by the CISO and is responsible for conducting security assessments on Web applications and Web sites to make sure they comply with the requirements identified within the Act, MD 210.12, and the ITPs. In addition to security assessments, OA/OIT/EISO will ensure that the (CA)^2 process is updated on an ongoing basis to ensure that it takes into account the latest cyber security threats to Web applications and Web sites. OA/OIT/EISO is also responsible for:

- Source Code Application Scans – In accordance with the (CA)^2 process, Web applications have to undergo a source code analysis to ensure that there are no application coding flaws that could be exploited by malicious actors to circumvent the application and network security protocols. As part the process, OA/OIT/EISO will review source code scan reports to make sure those applications don't have coding vulnerabilities.

Note: Upon request, OA/OIT/EISO will assist agencies in completing source code scans.

- Host-Based Intrusion Scans – All Web applications hosted on agency Web servers will have to provide OA/OIT/EISO with a copy of a current intrusion scan

report that shows that the host is secure, and the most recent patches are in place.

- Web Application Scans – While deployed in staging, Web applications are to undergo a Web application scan to show that the application security protocols are in place and functioning correctly. This report would be attached to the $(CA)^2$ submission and reviewed by OA/OIT/EISO to validate there are no medium or high vulnerabilities.

- Payment Card Industry Data Security Standard (PCI-DSS) – OA/OIT/EISO will assess Web applications that process credit cards to see if they comply with PCI-DSS and OA/OIT policies, procedures, and standards.

6.4 <u>Agencies</u> – Agencies developing or procuring Web applications have to complete the $(CA)^2$ process. In addition to completing the $(CA)^2$ process, agencies are responsible for:

- Appointing $(CA)^2$ POC – As part of the assessment process, agencies will appoint a primary and secondary point of contact to complete the $(CA)^2$ assessment process and to act as the liaison between the agency, OA/OIT/EISO, and the $(CA)^2$ review. For more information about the $(CA)^2$ POC roles and responsibilities, reference the section entitled *$(CA)^2$ Review Board, $(CA)^2$ Points of Contact (POC)*.

- Triennial Reaccreditation – Web applications are accredited for only three years. After three years, applications must undergo the reaccreditation process which means that agencies are to update the application information and complete the $(CA)^2$ risk assessment process.

- Compliance - Agencies will make sure that they comply with the policies, procedures, and standards identified in OA/OIT ITPs.

- Risk Mitigation Plan – Agencies that have applications that have risks that cannot be remediated will be required to submit a risk analysis, and risk mitigation plan to OA/OIT/EISO. This plan will identify and analyze the risks associated with the Web application and identify how the agency plans to mitigate those risks.

- Conditional Accreditation – Applications receiving conditional approvals will only receive 18-month grace period to remediate the vulnerability documented during the $(CA)^2$ risk assessment process. After this period, agencies will need to resubmit the application for a new risk assessment.

- Agency or Business Owner-Specific Security Requirements – The agency will be responsible for capturing any agency or business owner-specific security requirements not addressed in the OA/OIT ITPs.

6.5 <u>Office of the Budget, Comptroller Operations, Bureau of Audits (OB-BOA)</u> – OB-BOA is responsible for evaluating the risk and materiality impact of financial or fiscal-based applications and determining if further examination or assessment is warranted. In addition to this, OB-BOA will:

- $(CA)^2$ Review Board Representative(s) – The Director of OB-BOA is responsible for appointing members from the bureau to participate in the $(CA)^2$ process.

- Accounting and Financial Controls – OB-BOA is responsible for evaluating the soundness, adequacy, and relevance of controls related to accounting and financial applications.

6.6 Third-Party vendors, licensors, contractors, or suppliers – shall comply with the requirements as outlined in this ITP.

7. 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 210.12 *Electronic Commerce Initiatives and Security*
- ITP-BUS001 – *IT Planning and Projects*
- ITP-SFT000 – *Software Development Life Cycle (SDLC) Policy*
- ITP-SEC017 - *COPA Policy for Credit Card Use for e-government*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- Further, this policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-2, AC-3, AC-4, AC-7, AC-12, AC-25, AU-12, CA-1, CA-2, CA-3, CA-4, CA-6, CA-8, CM-2, CM-3, CM-4, IA-2, IA-6, IA-7, IA-8, IA-12, PM-17, RA-3, RA-5, RA-7, SA-10, SA-11, SA-15, SC-2, SC-3, SC-5, SC-20, SI-2, SI-12, & SR-4 Per Special Publication 800-53 R5.

8. Authority

- Executive Order 2016-06, *Enterprise Information Technology Governance*

9. 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 are to be directed to RA-ITCentral@pa.gov.

10. 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 is to 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	
Original	4/28/2009	Replaces ITB B.5 Security & Digital Certificate Policyand Encryption & Internet/Intranet Browser Standards fore-Government Web Sites & Applications	
Revision	12/23/2009	The policy had to be modified to meet new application hosting requirements identified by the Office of General Counsel.	
Revision	9/17/2010	Recertification has been changed to every three years	
Revision	8/16/2011	The scope was modified to clarify what applications need to go through the process, a new term called “At Risk Application” was added, and a new clause informing agencies that submissions not updated within one year of the initial submission will be automatically be removed from the (CA)^2 system.	
Revision	4/2/2014	ITP Reformat	
Revision	06/xx/2021	• Purpose updated to reference to NIST Alignment • Third party vendors added to Scope and Responsibilities • Definition for internet facing web application added • Removed PCI DSS Standards reference list, added reference to ITP-SEC017 (this contains reference to current PCI DSS standards) • Removed procedures (this will be moved to OPD) • Updated Related ITPs, Authority, Publication Version Control and Exemption sections	Revised IT Policy Redline <06/17/2021>