Information Technology Policy
Commonwealth Application Certification and Accreditation

Number ITP-SEC005	**Effective Date** October 1, 2021
Category Security	**Supersedes** All Prior Versions
Contact RA-ITCentral@pa.gov	**Scheduled Review** September 2024

1. Purpose

This Information Technology Policy (ITP) sets forth the guidance that agencies and the Enterprise Information Security Office (EISO) must adhere to when assessing a Web Application for potential vulnerabilities by establishing the policy and technical procedures for the Commonwealth Application Certification and Accreditation $(CA)^2$ Process. This process is a requirement of the Electronic Transactions Act, Act No. 69 of 1999, *73 P.S. § 2260.101, et seq.*(Act) and *Management Directive (MD) 210.12, Electronic Commerce Initiatives and Security* to ensure compliance when using, sending, receiving, and storing electronic records and electronic signatures.

2. Scope

This ITP applies to all departments, boards, offices, 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. Background

This policy documents compliance with Chapter 5 of the Act relating to governmental agencies. It sets forth the rules for the acceptance and use of electronic transactions by governmental agencies and directs all executive agencies to comply with the standards established by the Office of Administration (OA).

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, known as the $(CA)^2$ 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's (OA/IT) 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/IT to agency owned websites.

4. Definitions

Internet Facing Web Application: 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 a Commonwealth web server. This includes content generated from a data visualization or business analytics platform.

5. Policy

Agencies must complete $(CA)^2$ assessments on:

- All Web Applications, Application Programming Interfaces (APIs), Mobile Applications, or Web Application Frameworks (hereinafter referred to as a "Web Application") that provide government services or process Commonwealth Data.
- Web Application frameworks that have not been vetted through the $(CA)^2$ process. Please review *ITP-SFT009, Enterprise Software and Application Development Standards* for a list of approved Web Applications. Any derivation from approved Web Applications will require an IT policy waiver against ITP-SFT009.
- Hardware and virtual devices that host a Web Application, Web services, databases, etc.
- Agencies shall refer to *GEN-SEC005B, CA2 Applicability Decision Matrix* (*Authorized CWOPA user access only*) for the applicability of various scenarios depending on the type of data center, hosting environment, or computing service.

This policy shall not apply to Computing Services if the following conditions are met:

- The Web Application and its components are hosted by the vendor as outlined in *ITP-SEC040, Computing Services Provided by Service Organizations* (also refer to *GEN-SEC005B, CA² Applicability Decision Matrix*). 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.

5.1 Accreditation

Agencies that have a Web Application shall submit a $(CA)^2$ request to EISO for an accreditation review. This review consists of policy compliance, coding scanning and web vulnerability assessments. Agencies shall follow the procedures outlined in *OPD-SEC005A, Commonwealth Application Certification and Accreditation Procedures* (*Authorized CWOPA user access only*) when submitting a Web Application hosted within a data center or Commonwealth cloud instance (refer to GEN-SEC005B) for $(CA)^2$ accreditation. EISO may require an agency to prepare or resubmit a $(CA)^2$ request at any time.

Agencies who have a Web Application that receives a full accreditation shall ensure any changes to the security architecture are documented as outlined in section 5.4 (Accreditation Changes) of this policy to avoid any change in the status of their accreditation. In addition, agencies shall follow the procedures for reaccreditation as outlined in section 5.3 (Reaccreditation) to ensure continuous accreditation of their Web Application.

5.2 At Risk Applications & Conditional Accreditations

Any Web Application that goes through the accreditation process and has vulnerabilities that cannot be remediated prior to going into Production will be deemed as an "at risk application". In addition, a non-accredited or conditionally approved Web Application will also 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 or completed the $(CA)^2$ 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.

If deemed an "at risk application," the agency shall provide a Risk Analysis and Mitigation Plan, which includes probability and impact. The Risk Analysis and Mitigation Plan shall 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 shall be attached to the $(CA)^2$ submission and the Web Application shall be resubmitted for review. The plan will be reviewed and a determination made if the Web Application will be granted a conditional accreditation valid for a period of time consistent on the agreed upon plan. Additional details on conditional accreditations and Risk Analysis and Mitigation Plans can be found within *OPD-SEC005A, Commonwealth Application Certification and Accreditation Procedures*.

5.2.1 Conditional Accreditations

A conditional accreditation may only be granted for up to an 18-month grace period to allow the agency to remediate any vulnerability that was documented during the $(CA)^2$ process. The term of the grace period may vary but shall not exceed 18-months. Agencies shall ensure their Web Application is submitted for reaccreditation prior to the established grace period expiring.

If the agency does not submit for reaccreditation prior to its established grace period expiring, the Web Application will lose its conditional accreditation status and a new $(CA)^2$ request must be submitted.

No more than two (2) conditional accreditations will be granted per Web Application. Upgrades to the versioning of a Web Application will not reset the count of conditional accreditations. This is to ensure that vulnerabilities present on a Web Application are being addressed by the agency in a timely manner to prevent security issues.

5.3 Reaccreditation

An accredited Web Application shall be submitted for reaccreditation every three (3) years to maintain its security accreditation. Any changes to an accredited Web Application's security architecture will void its previous accreditation status. To regain $(CA)^2$ accreditation, agencies shall submit a new or updated $(CA)^2$ request. Refer to *OPD-SEC005A, Commonwealth Application Certification and Accreditation Procedures* for detailed requirements and procedures related to reaccreditations.

5.4 Accreditation Changes

Agencies shall ensure any changes to an accredited Web Application's security architecture or software bill of materials (SBOM), as listed below, are documented in the $(CA)^2$ system as a new submission or a modification to a previous $(CA)^2$ request to prevent the Web Application from becoming non-accredited.

- New or upgraded hardware platform.
- New or upgraded operating system, middleware component, or application.
- Changes to system ports, protocols, or services.
- Changes in data types processed, stored, or transmitted by the system.
- Changes to how data is processed (refer to *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data* to ensure data is properly identified, classified, and protected).
- Changes to cryptographic modules or services.
- Changes to security and/or privacy controls.

NOTE: If a Web Application becomes non-accredited, the agency shall initiate a new $(CA)^2$ request for the accreditation of the Web Application. Failure to do so will violate Commonwealth policy.

5.5 Security Requirements

In addition to the security requirements established by OA/IT ITPs, there may also be agency-specific security requirements that are not captured by OA/IT 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 (i.e., PCI, NIST, CJIS, IRS, etc.) 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.

5.6 Withdrawal from (CA)2

A Web Application that has started the $(CA)^2$ process but has not been updated within one year of the initial submission date shall be automatically withdrawn in the $(CA)^2$ system, and the Application Inventory will be updated. This is being

done to remove any Web Application that is not ready to begin the (CA)^2 process or has been cancelled and was not removed from the system.

Note: Submitters can avoid having a Web Application removed from the (CA)^2 system by submitting an updated status report in the system's comments field or by contacting the (CA)^2 Administrator.

5.7 Roles within the (CA)2 Process

Role	Role Requirements	Role Responsibilities
Review Board	• (CA)^2 Administrator • (CA)^2 Subject Matter Experts	• Determine if submitted Web application presents security threat to Commonwealth's IT infrastructure.
Administrator	• EISO Team Member	• Day-to-day administration of (CA)^2 system and process. • Addresses agency questions, comments, concerns, and issues. • Updates (CA)^2 system to address changes within OA/IT ITPs or security threats. • Entering and updating user accounts in (CA)^2 system. • Functions as coordinator of the Review Board and schedules meetings as needed.
Subject Matter Experts (SMEs)	Enterprise SMEs in the areas of: • Policy • Source code, or • Web Vulnerability (dynamic and host scans)	• Assist the EISO in the evaluation of (CA)^2 submissions. • Represent OA/IT in instances where clarification is needed, or agencies request technical assistance.
Point of Contact (POC)	• Agency application owner • Agency technical lead, or • Agency business owner	• Acts as the liaison between the agency, EISO, and the Review Board. • Ensure applicable Web Application is submitted through the (CA)^2 process every three (3) years to meet triennial reaccreditation requirements. • Contact the Administrator for (CA)^2 user updates/changes, requests for assistance with security scans, or to request a Review Board meeting.
Submitter	A Commonwealth employee from the submitting agency. • Role Preference: A project manager who understands security and Commonwealth policy.	• Submits and monitors (CA)^2 process for Web Application in accordance with policy procedures. • Updates Web Application information and resubmits through the (CA)^2 process if there are changes to the security architecture. • Provides business owners with updates on the status of applicable (CA)^2 submissions as they progress through the process.
EISO	EISO Team Member(s)	• Conduct security assessments as requested by Agencies.

Role	Role Requirements	Role Responsibilities
		• Update the (CA)^2 process in alignment with Commonwealth policies and current threat landscape. • Review source code scan reports to ensure applications do not have coding vulnerabilities. • Review host-based vulnerability scan reports to ensure the host is secure and most recent patches applied. • Review DAST scan reports to ensure there are no operational vulnerabilities.

Agency	• Submitter
	• POC
	• Information Security Officers
	• Agency application owner
	• Agency technical lead, or
	• Agency business owner
		• Appoint a primary and secondary POC.
		• Ensure completion of (CA)^2 for process agency Web Applications.
		• Ensure triennial completion of (CA)^2 required reaccreditation process for agency Web Applications.
		• Comply with policies, procedures, and standards in OA/IT ITPs, MDs, and applicable security frameworks (i.e., PCI, NIST, CJIS, IRS, etc.).
		• As requested, submit Risk Analysis and Mitigation Plans to EISO.
		• Follow up on any Web Application which receives conditional accreditation prior to expiration of grace period.
		• Capture agency or business owner specific security requirements not addressed in OA/IT ITPs.
		• Conduct Application and Host scanning and review reports to ensure vulnerabilities are not present and most recent patches are applied. If the agency has the proper tools and resources, scanning shall be conducted within the agency prior to EISO engagement. Scanning to include:
		  • Static Application Security Testing (SAST) and Source Code Analysis (SCA)
		  • Host-based Vulnerability Scans
		  • Dynamic Application Scanning Technology (DAST)

6. Responsibilities

6.1 Commonwealth Chief Technology Officer (CTO) shall:

Assist the CISO in completing the (CA)2 process on any Web Application being hosted on the Commonwealth network.

6.2 Commonwealth CISO shall:

- Oversee the staff or resource management of those tasked within EISO who

are responsible for monitoring compliance of the (CA)^2 process on an existing or prospective Web application.
- Fulfill the role of Final Reviewer by reviewing the status of all of (CA)^2 submissions and comments and making a recommendation to operate.
- Select a board of technical experts and security advisors to serve on the (CA)^2 Review Board.

6.2 (CA)2 Review Board shall:
Review (CA)2 requests to determine if they present security threats to the Commonwealth's IT infrastructure.

6.4 (CA)2 Administrator shall:
Be responsible for the day-to-day operations and system administration of the (CA)2 process. In addition, they will function as coordinator of the (CA)2 Review Board.

6.5 (CA)2 Subject Matter Experts (SMEs) shall:
Assist EISO in evaluating (CA)2 submissions and represent OA/IT in instances where clarification is needed, or agencies request technical assistance.

6.6 (CA)2 POC shall:
Act as the liaison between the agency, EISO, and the Review Board, obtain triennial reaccreditations, and work with EISO to ensure agency (CA)2 matters are addressed.

6.7 (CA)2 Submitter shall:
Be responsible for submitting and monitoring an agency's Web Application into the (CA)2 system, providing the agency status updates, and updating information.

6.8 EISO shall:
- Conduct security assessments as requested by an Agency on a Web Application to make sure it complies with the requirements identified within the Act, MD 210.12, ITPs and any applicable security framework (i.e., PCI, NIST, CJIS, IRS, etc.).
- Update the (CA)^2 process on an ongoing basis to ensure that it considers the latest cyber security threats to any Web Application.
- Review source code scan reports, host-based vulnerability scan reports and DAST scan reports in alignment with this policy to protect against vulnerabilities and ensure proper patching.

6.9 Agencies that are developing or procuring Web Applications shall:
Complete the (CA)^2 process per the procedures outlined in *OPD-SEC005A, Commonwealth Application Certification and Accreditation Procedures (Authorized CWOPA user access only)* for any Web Application hosted within a data center or Commonwealth Cloud instance (refer to GEN-SEC005B). In addition to completing the (CA)^2 process, agencies are responsible for the following:
- Appointing a POC
- Obtaining Triennial Reaccreditation
- Policy Compliance
- Submitting necessary Risk Analysis and Mitigation Plan(s)
- Follow-up on Conditional Accreditation(s)
- Capturing Agency or Business Owner-Specific Security Requirements
- Conducting Application and Host Scanning
- Ensuring that any Web Application being placed onto the Commonwealth

network is secure and potential vulnerabilities are either remediated or that a Risk Analysis and Mitigation Plan is in place.

6.10 Office of the Budget, Comptroller Operations, Bureau of Audits (OB-BOA):

May, upon request by an agency, provide audit response as possible risk mitigation techniques in accordance with *Management Directive 210.12, Electric Commerce Initiatives and Security*.

6.11 Third-Party vendors, licensors, contractors, or suppliers shall:

- Ensure all solution components are securely coded, vetted, and scanned.
- Obtain an independent third-party vulnerability assessment within the first six (6) months of Contract execution and such assessment shall be completed annually thereafter.
- Shall obtain an independent third-party vulnerability assessment more frequently as required to comply with regulations.
- Obtain an independent third-party vulnerability assessment upon request by the Commonwealth due to other warranted circumstances such as, but not limited to, a cyber security incident or a major change to the solution.
- Provide, at a minimum, an executive summary of any independent third-party vulnerability assessment results to the Commonwealth. Summary shall include at minimum, scan date, identified vulnerabilities, severity classification, remediation plan, and remediation status.

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 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 210.12, Electronic Commerce Initiatives and Security*
- *OPD-SEC005a, Commonwealth Application Certification and Accreditation Procedures* (*Authorized CWOPA user access only)*
- *GEN-SEC005B, CA^2 Applicability Decision Matrix*
- *ITP-BUS001, IT Planning and Projects*
- *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *ITP-SEC017, COPA Policy for Credit Card Use for e-Government*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC023, Information Technology Security Assessment and Testing Policy*
- *ITP-SEC024, IT Security Incident Reporting Policy*
- *ITP-SEC040, Computing Services Provided by Service Organizations*

- *ITP-SEC041, Commonwealth IT Resources Patching Policy*
- *ITP-SFT000, Software Development Life Cycle (SDLC) Policy*
- *ITP-SFT009, Enterprise Software and Application Development Standards*
- *Electronic Transactions Act (Act No. 69 of 1999)*
- *NIST CVSS Vulnerability Metrics*
- *MITRE's CWE ID Search*
- *MITRE's CVE ID Search*
- *Payment Card Industry Data Security Standards*
- *Executive Order 14028, Improving the Nation's Cybersecurity*
- *NIST Special Publication NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems*
- 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 shall 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 shall be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Policy Waiver Review Process* for guidance. The waiver shall be against this policy and include a list of any additional ITPs that the Web Application is non-compliant with and that require such a waiver.

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	4/28/2009	Replaces ITB B.5 Security & Digital Certificate Policy and Encryption & Internet/Intranet Browser Standards for Government Web Sites & Applications	N/A
Revision	12/23/2009	The policy had to be modified to meet new application hosting requirements identified by the Office of General Counsel.	N/A
Revision	9/17/2010	Recertification has been changed to every three years	N/A

Version	Date	Purpose of Revision	Redline Link
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 removed from the (CA)2 system.	N/A
Revision	4/2/2014	ITP Reformat	N/A
Revision	06/17/2021	• 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	N/A
Revision	11/2/2021	• Updated BOA responsibilities • Added links throughout policy	N/A
Revision	04/28/2022	• Internet facing web application definition updated to be consistent with OPD. • References to OPD added.	N/A
Revision	09/07/2023	• Purpose updated, additional language moved to Background/Policy Sections. • Scope updated consistent with connection to Commonwealth Network. • Background section created with language moved from Purpose. Additional content removed. • Policy updated to list Scope of what is encompassed in this policy (from previous Purpose language). • Criteria in scope of CA^2 has been expanding to include, intranet and extranet Web Applications, APIs, Mobile Apps and Web Application Framework – some language was in previous version but updating to encompass all. • Web Application is standard term now utilized in ITP and supporting documents to refer to items in scope of CA^2. • Reference added to ITP-SEC009 in policy language and Related ITPs/Other References to provide information on Web Application frameworks. • Creation of GEN-SEC005B CA^2 Applicability Decision Matrix and references added throughout document. • "Vendor hosted web applications" updated to "Computing Services." • Reference added to ITP-SEC040 and GEN-SEC005B for assistance in determining what is not applicable to CA^2. • Additional policy sections added to Accreditation, At Risk Applications & Conditional Accreditations, Reaccreditation, Accreditation Changes, Security Requirements, Withdrawal from CA^2, and Important Roles with the CA^2 Process. • Accreditation related policy language placed in section 5.1 – amended to added reference to OPD-SEC005A and align with current process/requirement. Additional policy language added regarding agencies documenting changes to Web Applications to ensure consistent accreditation. • At Risk Applications related policy language placed in section 5.1 – amended to current requirements/process.	Revised IT Policy Redline <09/07/2023>

Version	Date	Purpose of Revision	Redline Link
		• Conditional Accreditations created in section 5.2.1 – language developed to provide information on conditional process, requirements and restrictions. • Reaccreditation policy language moved to section 5.3 – amended to current requirements/process. • New section in 5.4 created for Accreditation changes. This outlines criteria which would affect a Web Applications accreditation and reminders users to their requirements. • Security requirements moved to section 5.5 – added examples of additional requirements agencies may have and removed bullet for PCI. • Withdrawal from CA2 (section 5.5) updated based on current requirements/process. • New section created in 5.6 for important roles in CA2 process. This streamlines information previously listed under the Responsibilities and provides a breakdown of all roles, who would fulfill who and the responsibilities of that role. • Section 6 Responsibilities was streamlined to policy defined requirements for each role involved in process. Third party vendor requirements were updated in alignment with ITP-SEC040 (Vulnerability Assessment CSR)	