1.0 PURPOSE

The purpose of this policy is to insure that the West Virginia Office of Technology (WVOT) validates the security readiness for devices, systems, application and system software, and other technology prior to deployment into a production status. This validation includes appropriate reviews and/or testing of configurations, hardening, functionality and compliance with specifications, regulations, standards and those objectives that were the basis for the initiative.

2.0 SCOPE

All technologies deployed, and all employees who are responsible for these deployments, within the scope of responsibility of the WVOT.

3.0 POLICY

3.1 This policy provides the framework for control activities needed during the development, building, testing, and implementation of devices, systems, application and system software, and other technology within West Virginia State Government.

3.2 Certification and Accreditation (C&A) requirements must be part of the life cycle for all devices, systems, application and system software, and other technology, unless excluded in writing by the CTO.

3.3 The C&A Process should be initiated before deployment, and where possible, before acquisition of the system.

3.4 Whenever information systems contain Federal Tax Information (FTI), or other sensitive information as defined by the WVOT Data Classification Policy, the agency must:

3.4.1 Manage the information system using a life cycle methodology that includes information security considerations.

3.4.2 Obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.

3.5 The four phases of the C&A process include: Initiation, Certification, Accreditation, and Monitoring.

3.6 Phase I: Initiation and Research

3.6.1 The initiation phase should be the first step in the C&A process. This phase helps organize and gather all relevant information in a manner that will allow agency decision-makers to thoroughly and accurately evaluate all risk associated with the system in question.

3.6.2 The information gathered in this phase will very between systems and devices, however most of the following information should be present in this stage of the C&A plan:

- **System Information**: The intent of the development or deployment of the system at a high level. Information about the system should include what it is; where it is supposed to be installed; vendor or product information; technical specifications or any other information that would need to be known to do proper research on the system.

- **System Requirements:** Categorizes any confidentiality, integrity and availability requirements; identification of known threats and/or vulnerabilities; and identifying initial risks (development and deployment), and ongoing risks (loss or compromise). Deployment owners must prepare appropriate materials and identify essential activities required to get devices, systems, application and system software, and other technology accredited for certification. Makes note of all security requirements.

- **System Justification:** Program and systems managers must define and document their business needs and requirements. Usually this information is available in the RFQ or RFP.

- **Responsible Parties:** Responsibilities for C&A must be assigned to the appropriate individual(s), and organizations will need to determine and define methods for implementing security requirements among identified stakeholders. This section identifies the stakeholders and the deployment (team) leader, including initiative sponsors. The **Certification** and **Accreditation Teams** should be identified in this phase.

    - **Certification Team** – Should be staffed from the agency's internal security team, WVOT's Information Security Office, or a combination of both.

    - **Accreditation Team** – Should be comprised of members from WVOT and the agency ultimately responsible for the system. The Accreditation Team should be formed by individuals that have the authority to modify the project timeline and priorities, if needed.

- **Time Frame:** Identifies the timeframe of the project or initiative (much of this could come from the project initiation documentation or charter),

- **Known Issues or Concerns:** Records all stakeholder agreement(s), or concerns(s), on the accreditation plan and certification criteria, and security requirements documentation.

3.7 All materials and information from Phase I should be passed on to the Certification Team for Phase II.

3.8 **Certification: Phase II**

3.8.1 The Certification Team will identify the security best-practices for the system, based on NIST guidelines or other industry standards.

3.8.2 The Certification team will create a security test and evaluation plan that includes:

3.8.2.1 Vulnerability testing and results.

3.8.2.2 Proposed risk and vulnerability assessment documentation; and

3.8.2.3 Proposed security certification and accreditation statements, addressing internal and external connections affecting the application or system, as needed.

3.8.3 When approved, the specified actions and activities to fulfill the Certification requirements are documented, and activities specified are incorporated into the project plan at points (milestones) in the development and/or deployment preparation and execution phases, as determined through stakeholder input and consensus. .

3.8.3.1 Appropriate testing is conducted and results documented. Additional testing may be required to complete Phase III.

3.8.3.2 Phase I materials must be updated as part of the Phase II verification, in order to get the initiative plan and documentation reconciled for final certification review, approval, and signoff by the Certifying Authority (CA).

3.9 The C&A Plan, which now includes Phase I and Phase II, should be reviewed by WVOT's Chief Information Security Officer (CISO), with concurrent review and requests for additional information or enhancement leading to approval by any impacted stakeholders.

3.10 **Accreditation: Phase III**

3.10.1 Accreditation is the culmination of the C&A process. At this point the certification plan, the testing, and the results are submitted for final accreditation review.

3.10.2 A completed C&A binder (or accreditation package) is forwarded by the certification (team) leader to the CA, or a C&A Board (C&AB) if designated. This package includes:

- The C&A Plan, updated from Phase II to reflect the findings of testing and other Certification activities.
- Actual Phase II details, testing results documentation, and any risk analysis documentation that includes final risk levels determined, and risk designated as residual risk, to be accepted and managed.
- Proposed "go-live" date and any rollout planning/scheduling documentation, and
- Signed recommendation of the certification (team) leader for approval to deploy.

3.11 The C&A binder (accreditation package) is reviewed by the CA. If satisfied that the C&A requirements are met, an accreditation statement of approval is issued by the CA. The CA, unless otherwise designated by the WVOT CTO, is the WVOT CTO.

3.12 The accreditation statement of approval, issued by the CA, permits deployment of the system, application or system software, or other technology.

3.13 **Monitoring: Phase IV**

3.13.1 Once a device, system, application and system software, or other technology is formally accredited, the life-cycle of the deployed technology must be monitored to ensure that all applicable standards are maintained.

4.7.1.1 Changes to devices, systems, application and system software, or other technologies must be documented and analyzed for security impact, with appropriate remediation of findings of adverse security impact.

3.13.1.1 Every 3 years, or when major changes occur in software and/or hardware (whichever occurs first), responsible parties will be required to update the C&A documentation, to gain re-accreditation of the device, system, application and system software, or other technology.

3.14 **Pre-existing deployments of devices, systems, application and system software, and other technology:**

3.14.1 Devices, systems, application and system software, and other technology currently deployed must be identified, and are subject to a risk assessment review to assure that they do not pose unacceptable risk within the State of West Virginia technology environment. At the request of the CTO, or CISO, a C&A requirement may be imposed on any pre-existing technology.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 DEFINITIONS

6.1 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

6.2 Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

6.3 Certification and Accreditation (C&A) – Validation process that insures that the West Virginia Office of Technology validates the security readiness for devices, systems, software, and other technology prior to deployment of technology into a production status. This validation includes appropriate reviews and/or testing of configurations, hardening, functionality and compliance with specifications, regulations, standards and objectives the generated the deployment activities.

6.4 Authentication – The process of verifying the identity of a user.

6.5 Confidential Data – Information that is legally protected (e.g: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

6.6 Certification - Certification is an evaluation process assessing non-technical and technical security management, operations, and technical controls, policy, and requirements. Together with a risk analysis and a vulnerability assessment, certification produces documents that support management decisions.

6.7 Information Resources – All information assets, in all known formats.

6.8 Information Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

6.9 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State information security policies and procedures. The ISA is the agency's internal and external point of contact for all information security matters.

6.10 Procedure – A set of instructions or process steps prescribed in sufficient detail in order to understand how to meet a policy requirement. Procedures should document roles, methods, options, and examples necessary for a reader to understand how to comply with a policy.

6.11 Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

6.12 Security Contact – These individuals include the ISA or the ISL.

6.13 Threat – Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of information security.

7.0 Change Log History

- January 30, 2015 –
  - Added Appendices A and B; Clarified and reorganized sections on Phase I and Phase II.
- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions;
- 9/1/2016 – Policy Reviewed. No edits made.
- 10/20/2017 – Policy Reviewed. No edits made.
-

Below is a sample outline for common parts of a Certification and Accreditation Plan:

PHASE I

System Information

System Requirements

System Justification

Responsibilities

Time Frame

Known Issues or Concerns

Technical Testing Plan

PHASE II

Relevant Security Controls

Test Results

Re-Testing and Results

Discussion Notes and Documentation about Known Risks

Proposed Mitigation & Recommendations

Certification Statement

PHASE III

Documentation of Acceptable Risks

Stipulations and Requirements

Accreditation Statement

Certification and Accreditation Statements should be signed by the appropriate authority.

Security Certification Statement

The following recommendations must be considered before the Unity Communication and Messaging System is certified:

1. It is the recommendation of the Security Group that the Agency complete *Task X* before going live.

2. Vulnerability scans should be conducted every *X years/months/days*.

3. Other concerns.

Risk Accreditation Statement

During the Certification Process, the following vulnerabilities and/or risks were discovered.

Vulnerability #1

Description of issue.

Risk Level:

Vulnerability #2

Description of issue.

Risk Level:

At the time of this C&A Plan, the residual risks associated with the continued operation of the Unity Connection Cluster are acceptable and the system is granted approval to operate until FY2019 (3 years) without being recertified