1.0 PURPOSE

The West Virginia Office of Technology (WVOT) will maintain an objective and internally independent Information Security Audit Program. This program will serve the Executive Branch by examining, evaluating, and reporting on information technology (IT) applications, related systems, operations, processes, and practices to provide reasonable assurance that security controls will:

- Safeguard information assets and protect privacy;
- Preserve the integrity and reliability of data;
- Function as intended to achieve the entity's objectives; and
- Comply with established and/or relevant standards, policy, and regulations.

Audit efforts are focused on areas presenting the highest degree of risk, as well as on those areas where risk mitigation will provide the greatest potential benefit to the Executive Branch. This policy explains the authority of the WVOT Information Security Audit Program, as well as the standards of audit practice.

2.0 SCOPE

This policy applies to all State entities or personnel who desire or require auditing services from the WVOT Information Security Audit Program, unless classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Instant Messaging services.

3.0 POLICY

3.1 All WVOT IT Auditors are bound by confidentiality standards, and are required to sign the Department of Administration Confidentiality Statement annually.

3.2 The public's right to the transparency of government information must maintain a balance with the proper use of that information. In addition, many government programs are subject to laws and regulations dealing with the disclosure of information. To accomplish the balance, all WVOT IT Auditors will:

3.2.1 Read and understand all WVOT Policies.

3.2.2 Exercise discretion in the use of information acquired in the course of duties in achieving this goal.

3.2.3 NOT improperly disclose information to third parties under any circumstances.

3.3 Audit reports and requests involving Federal Tax Information (FTI) will be maintained for five (5) years or the applicable records control schedule, whichever is longer.

3.4 Agencies must ensure that audit information is archived for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. This enables the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.

3.5 Internal audit reports are exempt from disclosure under the West Virginia Freedom of Information Act (West Virginia Code §29B-1-4).

3.5.1 Due to the sensitive data that audit reports typically contain, the distribution of audit reports should be restricted to only personnel with a business need for the information. Examples of exemptions include:

3.5.1.1 Passwords

3.5.1.2 IP addresses

3.5.1.3 Modem phone numbers

3.5.1.4 Critical infrastructure information

3.5.1.5 Records containing specific or unique vulnerability assessments

3.5.1.6 Response plans or disaster recovery plans

3.5.1.7 Risk assessments, tests or the results of those tests, etc.

3.5.2 The cover page should contain the words "Not Subject To FOIA" The Information Security Audit Program has the authority to require that a Non-Disclosure Agreement be signed prior to providing any reports to the client.

3.5.3 Based on the technical responsibility of the client, The Information Security Audit Program may deem it appropriate to provide a summary report that does not contain raw data, such as scan results or technical configurations. The Information Security Audit Program may use their discretion to redact data elements.

3.6 Information collected during an audit will only be used for official purposes and not for personal gain, in a manner contrary to law, or detrimental to the legitimate interests of the audited entity or the audit organization. This includes the proper handling of classified information or resources as defined in the WVOT Data Classification Policy.

3.7 The WVOT Information Security Audit Program is responsible for providing the following to its customers:

3.7.1 Objective, internally independent examination of security controls pertaining to systems, operations, processes, and practices;

3.7.2 Validation that security controls are:

3.7.2.1 Protecting privacy and safeguarding information assets;

3.7.2.2 Preserving the integrity and reliability of data; and

3.7.2.3 Operating in accordance with standards, policy, and regulations.

3.7.3 Report threats and vulnerabilities found, including unexpected items and/or situations detected during the audit.

3.7.4 Provide recommendations to mitigate or resolve risk as identified in the audit findings.

3.8 During the period of the audit engagement, in order to obtain accurate and complete information, perform thorough evaluations, and prepare meaningful reports, WVOT Information Security Audit personnel will:

3.8.1 Prepare an engagement memo for the customer with details of audit objectives, scope, and schedule;

3.8.2 Acquire and maintain complete access, on a need to know basis, to records, property, computer systems, functions, and personnel;

3.8.3 Allocate resources, establish schedules, select subjects, determine audit scope, and apply the techniques required to achieve engagement objectives; and

3.8.4 Obtain the necessary assistance of personnel within the units/functions of the agency where they provide services.

3.9 Prior to internal audit engagements, entities/customer must read, agree to comply with, and sign-off on an engagement memo, all provisions of this policy, and WVOT-PR1008, the *Information Security Audit Program* procedure.

3.10 The draft engagement findings and recommendations will be forwarded to the client Director.

3.11 The delivery of the final engagement findings and recommendations will be limited to the CTO, the CISO, the client Director, and other parties as authorized.

3.12 The Information Security Audit Program will only release specific information, engagement findings and recommendations to additional entities under the following circumstances:

3.12.1 by request from the audit client,

3.12.2 for peer review, and/or

3.12.3 under order of subpoena.

3.13 Information Security Audits may be scheduled in relationship to the following:

3.13.1 Scheduled at least three (3) to six (6) months in advance (see WVOT-PR1008);

3.13.2 On an ad-hoc basis;

3.13.3 As a client special request;

3.13.4 Post incident; or

3.13.5 As a risk assessment;

3.14 Standards of Audit Practice

3.14.1 The WVOT Cyber Security Office (CSO) has undertaken the establishment, maintenance, and management of an internal Information Security Audit Program.

3.14.2 The WVOT Information Security Audit Program follows the Professional Standards of the Practice of Internal Auditing as issued by the Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), the National Institute of Standards and Technology (NIST) and the International Information Systems Security Certification Consortium (ISC^2)

3.14.3 The WVOT Audit Program adheres to information security standards as published by the Information Standards Organization (ISO).

3.15 Audits may be requested by agencies, initiated by WVOT, or originate by third parties.

3.16 Audits Engaged by Third Parties

3.16.1 Agencies engaged in any IT audit activity by third parties (Ex. IRS) are responsible for contacting the WVOT CSO Audit Team as soon as notification of the audit has been received.

3.16.2 The WVOT Information Security Audit Program will synchronize third-party information security audit activities with WVOT services and units. This coordination will:

3.16.2.1 Determine that audit objectives are clearly defined, and then achieved upon completion. This will include a review of the engagement memo;

3.16.2.2 Ensure that appropriate and accurate information is provided to third-party auditors;

3.16.2.3 Avoid duplicate audits and control audit costs;

3.16.2.4 Ensure that operating units cooperate fully with the third-party auditors;

3.16.2.5 Coordinate communications between Executive Branch personnel and third-party auditors including, but not limited to audit findings and recommendations;

3.16.2.6 Review engagement findings and recommendations; and

3.16.2.7 Facilitate effective follow-up activities and monitor progress in addressing audit recommendations.

3.16.3 Third-party auditors may be required to follow additional and/or more stringent standards and procedures than those mandated by the WVOT.

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 POLICY-SPECIFIC DEFINITIONS

6.1 Information Security Audit Program - The types of audits performed by the Program include, but are not limited to the following: (1) Applications and systems; (2) Data centers /sites; (3) Data management; (4) Internal technology controls; (5) Investigative and incident follow-up; (6) Mobile and portable devices; (7) Networks and network components; (8) Physical security; (9) Policy and regulatory compliance; (10) Telecommunications; and (11) Technology operations. CSO Auditors serve the Executive Branch by examining, evaluating, and reporting on IT applications, systems, operations, processes, and practices to provide reasonable assurance that security controls:

- Safeguard information assets and protect privacy
- Preserve the integrity and reliability of data
- Function as intended to achieve the entity's objectives
- Operate in accordance with standards, policy, and regulations

6.2 Information Systems Audit and Control Association (ISACA). An International professional organization that establishes standards for the practice of Information Technology Auditing. ISACA also manages certification/licensing exams, continuing education for Certified Information Security Auditors, Certified Information Security Managers and other security professionals. ISACA is a global organization for information governance, control, security and audit professionals.

6.3 Institute of Internal Auditors (IIA) – An international professional association, which is recognized throughout the world as the internal audit profession's leader in certification, education, research, and technical guidance. The mission of the association is to provide dynamic leadership for the global profession of internal auditing. Members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

6.4 Integrity - Protecting data from unauthorized or unintentional modification or deletion.

6.5 International Information Systems Security Certification Consortium (ISC²) -The International Information Systems Security Certification Consortium, Inc. [(ISC) ²] is a not-for-profit organization incorporated under the laws of the Commonwealth of Massachusetts and the U.S. Internal Revenue Code. As such, all credential holders in good standing are considered members of (ISC) ². (ISC) ² is charged with the responsibility for maintaining the (ISC) ² CBK®, a compendium of industry best practices for information security, including those for CISSPs, SSCPs, and CAPs. The CBK is a critical component for certifying the minimum acceptable competence for professionals seeking to hold various credentials. (ISC) ² also provides the information security community with education seminars, examinations and related services. In addition, (ISC) ² acts to safeguard certification standards, and participates in information security conferences, etc., as some of its more important activities.

6.6 Three-Year Security Audit Plan – A rolling plan developed by the Information Security Audit Program to schedule audits and select audit targets. This plan will be reviewed and approved annually by the Chief Information Security Officer (CISO).

7.0 Change Log History

- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions;
- 09/01/2016 – Reviewed policy. Minor text changes to clarify language in section 3.16
- 8/12/2017- Reviewed policy. Minor text changes
- 10/20/2017- Reviewed policy. Minor text changes