

**Office of the Chief Information Officer
Enterprise Policy**

Policy Number: CIO-091

Effective Date: 10/07/2013

Reviewed Date: 11/05/2014

Subject: Enterprise Information Security Program Policy

Policy Statement: The Commonwealth Office of Technology (COT) is charged with ensuring the confidentiality, integrity, and availability of the Commonwealth's computing environment. [KRS 42.724](#) gives the Office of Chief Information Security Officer (CISO) the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities. Therefore, this policy has been created to align the Commonwealth's Enterprise Information Security Program with the security framework of the current National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls. The implementation of the controls within the NIST framework will vary to some degree across the enterprise based on the system classification and risk. The baseline security controls will start with a moderate impact. The baselines are a starting point from which controls can be removed, added or specialized based on requirements. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate.

A framework is a comprehensive information security model that ensures the overall security of information by not only focusing on the technological issues but also addressing other principal elements such as people, processes and business strategies. The purpose of this policy to provide a security framework to create security safeguards, best practices and standards. This policy also offers a dynamic security plan to protect the Commonwealth's Infrastructure and critical assets.

Policy Maintenance: The Office of the Chief Information Security Officer shall be responsible for maintaining this policy. Agencies may choose to add to this policy, in order to enforce more restrictive internal policies as appropriate and necessary. Therefore, staff members are to refer to their agency's security policies, which may have additional information or clarification of this enterprise policy.

Authority: KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies that support and promote the effective application of information technology within the executive branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

Applicability: This policy is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, vendors, and other workers within the Executive Branch agencies.

Responsibility for Compliance: Each agency shall be responsible for ensuring staff members within their organizational authority are aware of the provisions of this policy and that compliance by the staff member is expected. It shall be each Executive Cabinet's responsibility to enforce this policy.

Review Cycle: This policy will be reviewed at least every two years.

Policy: The Enterprise Information Security Program Policy establishes the overarching framework and provides guidance on matters affecting information security. By utilizing NIST Special Publication 800-53 as a base framework this enables and defines policies and controls within 18 areas which cover technical,

operational, and managerial controls that will meet State, Federal, and Agency requirements such as HIPAA, IRS and Payment Card Industry Data Security Standard.

The appropriate application of protective security ensures the operational environment necessary to conduct Commonwealth business in a confident and secure manner. Managing IT security risks allows agencies the ability to balance business need, cost, and effectively provide the necessary protection of the Commonwealth's people, information and assets commensurate with the level of assessed risk. The establishment of the Enterprise Information Security Program provides clearly defined, measurable, and enforceable security controls that will be consistently applied at an enterprise level to achieve these goals.

Maintaining compliance with this policy shall be the result of risk assessment practices in addition to regulatory audits, internal reviews and management oversight. With these results there can be measurement of effectiveness along with providing strategic direction.

Adoption of this common framework and its controls for the Commonwealth offers several advantages that include agencies sharing a common vocabulary and common set of concepts related to information security controls, which will improve communication and understanding with and among the agencies. Other advantages include common standards for auditing and common methods for compliance monitoring and greater insight into the overall security posture of the Commonwealth.

NIST 800-53, defines policies and controls within the 18 control principle families:

Control Principle Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authentication
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management

These control families are defined in greater detail in NIST Special Publication 800-53, Appendix F - *Security Control Catalog*. In areas that require further refinement to ensure applicability to Commonwealth business needs, additional guidance can be found in supplemental policies such as CIO-090, *Information Security Incident Response Policy*.

References:

- Federal Information Processing Standard (FIPS) 199
<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- KRS 42.724
<http://www.lrc.ky.gov/KRS/042-00/724.PDF>
- National Institute of Standards and Technology
<http://www.nist.gov/index.html>

- NIST Special Publication 800-53 release 4
Security and Privacy Controls for Federal Information Systems and Organizations
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- NIST Special Publication 800-60
Guide for Mapping Types of Information and Information Systems to Security Categories
http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
- Enterprise Architecture and Standards
<http://technology.ky.gov/governance/Pages/architecture.aspx>
- Enterprise IT Policies
<http://technology.ky.gov/governance/Pages/policies.aspx>

END