Policy Title and #	CIO-093: Risk Assessment				
Effective Date:	11/29/2016	Revision Date:	01/10/2019	Review Date:	04/21/2021

POLICY STATEMENT:
This policy establishes controls related to Risk Assessment. The controls outlined below detail the measures that must be implemented to protect Commonwealth information technology systems from the likelihood of avoidable threat or risk events and the consequences thereof. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

DEFINITIONS:
Availability: Ensuring timely and reliable access to and use of information.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Consequence: The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Integrity: Guarding against improper information modification or destruction.

Likelihood: The probability or frequency of something happening.

Risk: The chance of something happening, which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.

Risk Assessment: The overall process of risk analysis and risk evaluation.

Risk Management: The process of conducting planning, identification, analysis, response planning and the controlling of risk.

Risk Treatment: The selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:

- Avoid the risk – eliminate the opportunity for the risk to occur by changing whatever causes the potential for the risk
- Reduce the likelihood of occurrence – change processes or products to limit the chance the risk may occur
- Reduce the consequences of occurrence – change processes or products to limit the impact the risk may have
- Transfer the risk – shift the impact to a third party (insurance, warranties, guarantees, etc.)
- Retain/accept the risk – acknowledge the risk and opt not to take any action unless the risk occurs.

Risk Management Process: The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, as well as monitoring and communicating risk.

Significant Change: Any change to the information system that greatly alters the way that the system

obtains, stores, disseminates, or processes data or is a change to the foundation infrastructure that the system operates within such as hardware or operating systems.

System Security Plan (SSP): A list of security and operational controls maintained for a specific system that identified how the system and data will be protected within a framework dictated by state, federal, or business compliance needs.

Threat: Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations or the Commonwealth through an information system via unauthorized access, destruction, disclosure or modification of information and/or denial of service.

POLICY:
Agencies shall categorize the information systems within their control in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Agencies shall assign a Security Categorization (SC) and document the security categorization results, including supporting rationale, in the SSP for the information system. Agencies shall ensure that the authorizing official or designated representative reviews and approves the security categorization decision. A system's SC is represented as a composite of the potential impact (low, moderate, high, or not applicable) associated with each of the three security objectives for information and information systems such as:

SC (System name) = {(confidentiality, impact), (integrity, impact), (availability, impact)}

More detail on information system security categorization can be found in Federal Information Processing Standard (FIPS) 199.

Each agency shall conduct a risk assessment, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Agencies shall document the risk assessment results, review risk assessment results at least annually, disseminate the risk assessment results to the appropriate personnel, and update the risk assessment at least every three years or whenever there are significant changes to the information system or environment of operation. This includes the identification of new threats and vulnerabilities or other conditions that may affect the security state of the system.

Details on conducting a risk assessment are in SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments* and NIST Special Publication 800-30, Revision 1.

Agencies shall request a vulnerability scan against their information systems and hosted applications on a schedule based on federal, state, or business compliance needs for all systems, or when new vulnerabilities potentially affecting the system or applications are identified and reported. Agencies shall submit the request to the Commonwealth Service Desk via e-mail at CommonwealthServiceDesk@ky.gov.

Agencies shall analyze the vulnerability scan reports and results from the security control assessments and remediate legitimate vulnerabilities in accordance with an organizational assessment of risk. Agencies shall share information obtained from the vulnerability scanning process and security control assessments with the appropriate agency staff to help eliminate similar vulnerabilities in other information systems.

AUTHORITY:
KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

APPLICABILITY:
All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

RESPONSIBILITY FOR COMPLIANCE:
Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

MAINTENANCE:
COT's Office of the CISO has responsibility for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

REVIEW CYCLE:
COT's Office of the CISO will review this policy at least every two years.

REFERENCES:
Helpful references can be found on the Enterprise IT Policies webpage.