CITY OF HOUSTON

Administrative Procedure

Subject: **Cybersecurity Program**	A.P. No: **8-2**
	Effective Date: **October 17, 2014**

1. AUTHORITY

1.1 Article VI, Section 7a, City Charter of the City of Houston.

2. PURPOSE

2.1 To establish and implement a Cybersecurity Program based on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and the State of Texas Statewide Enterprise Security Framework.

2.2 To set the ground rules under which the City shall operate and safeguard its information and Information Systems to reduce the risk and minimize the effect of security Incidents.

3. OBJECTIVES

3.1 To establish a Cybersecurity Framework (Framework) that provides a common language for expressing, understanding, and managing cybersecurity risk, both internally and externally. The Framework will be used to help identify and prioritize actions for reducing risk and is a tool for aligning policy, business, and technological approaches to managing that risk.

3.2 To utilize the City's Framework to implement and maintain the following methodologies:

3.2.1 Describe the current state of cybersecurity within individual departments and the City as a whole.

3.2.2 Describe the target state of cybersecurity within individual departments and the City as a whole.

3.2.3 Identify and prioritize opportunities for improvement. Facilitate continuous improvement and assess progress toward the target state.

3.2.4 Develop and maintain a communications plan for internal and external stakeholders.

4. SCOPE

4.1 All City departments and divisions are required to adhere to this procedure.

5. DEFINITIONS

Authorization to Operate – The formal acceptance, by an Authorizing Official, that the security of an Information System's operation is commensurate with the risk and magnitude of harm resulting from a compromise of that system's confidentiality, integrity, and availability.

Authorizing Official (AO) – The official with the authority to formally assume responsibility for operating an Information System at an acceptable level of risk to organization operations (including mission, functions, image, or reputation), agency assets, or individuals. The AO is typically someone who is a primary stakeholder for the system being authorized.

City Information – Any data which is collected, generated, maintained, or controlled by or on behalf of the City.

Incident – Any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality.

Information Security – The protection of an Information System's confidentiality, integrity, and availability.

Information System – A discrete set of resources designed and implemented for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

6. OVERVIEW

6.1 The Framework is an objective-based approach to developing the Cybersecurity Program. It consists of standards, best practices and measurements that are presented in a manner that allows for consistent communication of cybersecurity risk within and across the City's departments, from the senior executive level to the implementation/operations level.

6.1.1 The five primary functions of the Framework, which will provide a high-level, strategic view of the City's management of cybersecurity risk are:

6.1.1.1 Identify

6.1.1.2 Protect

6.1.1.3 Detect

6.1.1.4 Respond

6.1.1.5 Recover

6.1.2 The Framework also identifies underlying key categories and subcategories for each of the above functions and matches them with existing standards, guidelines, and practices for each subcategory. This structure ties the high-level strategic view, outcomes and standards-based actions together for a cross-department view of cybersecurity activities (see Appendix A).

6.1.3 The City has established 21 distinct security categories within the primary functional areas. These 21 categories comprise the minimum components of the Citywide Framework (see Appendix A).

7. RESPONSIBILITIES

7.1 The overarching roles and responsibilities related to the City's Cybersecurity Program are defined in E.O. 1-48, Information Technology Security. Specific roles and responsibilities related to the implementation of the Framework are referenced throughout the remainder of this procedure.

7.1.1 Throughout this document, roles and responsibilities are generally listed at the highest level possible, with the operating assumption that specific tasks and functions may be delegated as necessary unless explicitly prohibited.

7.1.2 Department Directors shall be designated as Authorizing Officials for IT systems under their purview.

7.1.3 The Chief Information Officer (CIO) shall:

7.1.3.1 Issue City IT Requirements (CITRs) documents to keep the City Cybersecurity Program current with changes in the information Security environment and with changes in federal, state, and City laws, policy and guidelines, as needed.

7.1.3.2 Report periodically to the IT Governance Board and the Mayor on the effectiveness of the City's information security program, including the progress of remedial actions.

7.1.3.3 Ensure the development and maintenance of a Citywide Information System inventory.

7.1.4 The Chief Information Security Officer (CISO) shall:

7.1.4.1 Develop target state standards and metrics for City departments.

7.1.4.2 Direct the Current-State self-assessment by City departments using the Framework (see Appendix A).

7.1.4.3 Facilitate the gap-analysis of Current-State self-assessments and CISO-developed target state standards with City departments.

7.1.4.4 Facilitate progress toward target state and regular assessments of progress with City departments.

7.1.4.5 Ensure the Framework is implemented throughout the City.

7.1.4.6 Interact with internal and external resources to coordinate information security compliance across the City.

7.1.4.7 Ensure that the City develops, disseminates, reviews annually, and appropriately updates policy, procedure, and technical documentation as related to information and cybersecurity in accordance with federal, state and City requirements, E.O. 1-48, Information Technology Security; this procedure; and all related policies.

7.1.4.8 Establish and maintain a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in the City's Cybersecurity Program.

7.1.4.9 Authorize City IT Security policies.

7.1.4.10 Publish and maintain information security policies which will provide detailed information and guidance regarding the processes to meet the requirements of this administrative procedure.

7.1.5 The Department Directors shall:

7.1.5.1 Formally assume the responsibility for the cybersecurity of Information Systems operated within their Department (i.e. non-enterprise systems).

7.1.5.2 Allocate sufficient resources to adequately protect information and Information Systems based on an assessment of departmental risks.

7.1.5.3 Assign an AO Designated Representative(s) (AODR) as necessary. Note: The responsibility of signing an Authorization to Operate may not be delegated.

7.1.6 The AODR shall execute the responsibilities of the AO as delegated.

7.1.7 If designated by the department director, the Department Chief Technology Officers (CTOs), Assistant Directors of IT, and Deputy CIOs shall:

7.1.7.1 Ensure that the Framework is implemented according to a thorough assessment using the Framework categories and metrics (see Appendix A).

7.1.7.1.1 Conduct Current-State self-assessment using the Framework categories and metrics (see Appendix A).

7.1.7.1.2 Compare the current state to the target state and document the gap analysis with tactical plans and timelines for progress toward the target state, in collaboration with the CISO.

7.1.7.1.3 Continuously improve cybersecurity within the department and report progress to the CISO.

7.1.7.2 Provide necessary assessment documentation, as required.

7.1.7.3 Take appropriate actions to identify, and minimize or eliminate Information System security deficiencies and weaknesses.

7.1.7.4 Allocate resources to protect information and Information Systems based on an assessment of system risks.

7.1.7.5 Communicate feedback to the CISO, and AO regarding the impact of citywide information security requirements on the operation of their Information Systems.

7.1.7.6 Utilize, to the extent possible, City provided infrastructure

8. ATTACHMENT

8.1 Appendix A - Citywide Cybersecurity Framework

Appendix A
Citywide Cybersecurity Framework

Appendix A

Citywide Cybersecurity Framework*

Risk = ((Vulnerability * Threat) / Counter Measure)) * Asset Value
Risk is the potential of loss resulting from a given action, activity and/or inaction
Vulnerability refers to the inability to withstand the effects of a hostile environment
A **threat** is an act of coercion wherein an act is proposed to elicit a negative response
An **electronic countermeasure** (**ECM**) is an electrical or electronic device designed to trick or deceive

Function	Category	Methodology
Identify	Asset Management	Inventory and track devices, network components, applications, and workforce
	Business Environment	Identify and prioritize mission, objectives and activities to support risk decisions
	Governance	Identify policies, procedures and processes to manage and monitor risk
	Risk Assessment	Assess risk to organization, assets and individuals resulting from operation of information systems periodically
	Risk Management	Identify the assumptions, constraints, risk tolerance and priorities / trade-offs to support operational risk decision
Protect	Access Control	Limit facility and information/transaction access to authorized users or devices
	Awareness Training	Train personnel and partners on security responsibilities
	Data Security	Protect information and records from natural and man-made hazards
	Information Protection Process and Procedures	Implement security planning policies and procedures to ensure adequate protection
	Protective Technology	Implement technical security solutions that supplement processes and procedures to ensure cyber security and resilience
Detect	Anomalies and Events	Detect anomalous activities and determine impact
	Security Continuous Monitoring	Track, control and manage cyber security aspect of development and operation to identify cybersecurity events
	Detection Process	Implement and test detection processes to ensure timely and adequate awareness of anomalous events
Respond	Response Planning	Implement the agreed-upon steps and actions to meet risk objectives upon detection of cybersecurity events
	Communication	Coordinate response with internal and external stakeholders
	Analysis	Investigate anomalies, conduct an impact assessment, perform forensics and classify the incident
	Mitigation	Contain and eradicate the incident and strengthen controls to prevent reoccurrence
	Improvement	Incorporate lessons learned into plans and update response strategies
Recover	Recovery Planning	Execute recovery plan
	Improvements	Incorporate lessons learned into plans and update recovery strategies
	Communications	Communicate with public, media as needed to recover reputation

* Based on NIST – (National Institute of Standards and Technology)