Information Technology and Security Charter

The City of Baltimore ("City") is committed to responsible stewardship of the City's information technology (IT) resources. This includes preserving the confidentiality, integrity, and availability of all forms of information used by the City and maintained on behalf of all stakeholders including our residents, City employees and contractors, customers, vendors, non-profits, and other government entities. This Policy functions as an IT and Security Charter that will improve our ability to serve the community, strengthen the protection of data entrusted to the City by all individuals and entities, and mitigate the impact of future cyberattacks. The purpose of this IT and Security Charter is to define the responsibilities for developing, maintaining, and monitoring compliance with the City of Baltimore Information Technology and Security Manual (ITSM).

The City is committed to the secure operation of critical infrastructure as defined by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA) including, public health systems, public safety systems, water and wastewater systems, the operation of three dams, and government and commercial facilities.

The City enters into agreements with suppliers, vendors, software as a service (SaaS) providers and professional services that are used to maintain the City's infrastructure, protect the public and to provide resident services. The City is committed to protecting any sensitive data that is shared or hosted by these suppliers, vendors, Software as a Service (SaaS) or professional services providers.

The foundation of a mature IT program is a set of documented standards that describe how systems will be procured, developed, tested, implemented, and maintained. The standards provide minimum requirements that shall be used for system procurement, development, deployment, and operations. Documented IT Standards improve the City's ability to deploy cost effective systems in a predictable and timely manner, reduce the cost of operations and maintenance and improve our security posture. The Baltimore City Information Technology and Security Manual (ITSM) will be comprised of a set of IT Standards to manage IT assets and information effectively, efficiently, and securely on behalf of our residents and stakeholders.

I. SCOPE

This Policy applies to the City's computing, networking, digital technology, operational technology (OT), supervisory control and data acquisition (SCADA), telephony, digital assets and digital files, hardware, software, web applications, commercial off the shelf (COTs) applications, infrastructure or platform or software as a service (cloud IT), vendor managed IT or applications, workstations, desktops, laptops, tablets, the internet of things (IOT) devices, or information that may be owned, leased, entrusted to or managed by the City (hereinafter referred to as "IT resources").

This Policy applies to all users of IT resources owned, operated, or managed by the City to the extent allowed by law or applicable contracts. Individuals covered by this Policy are collectively

referred to as "users" and include but are not limited to full and part time employees, and, to the extent allowed by law or applicable contracts, the contractors, interns, partners, visitors, and customers that use the IT resources. The term "users" also applies to individuals who connect to the City's IT resources by wire or wirelessly using personally owned devices.

II. INFORMATION TECHNOLOGY AND SECURITY MANUAL (ITSM)

The Information Technology Security Manual (ITSM) is managed by Baltimore City Information Technology. The ITSM will provide a process for Agency review and comment prior to the adoption of new standards or updates to existing standards. The City's CIO and selected Senior Leadership from the Mayor's Office and Agencies will provide final review and approval.

The ITSM will cover the following sections:

- Authority, Governance, and Exception Process
- IT Security Standards
- Network, Desktop, and Server Standards
- Web, Application, and Database Development Standards
- Supervisory Controls and Data Acquisition (SCADA) Operational Technology Standards
- Telecommunication Standards

III. ROLES AND RESPONSIBILITIES

All users are responsible for following the Standards in the ITSM as well as the City's IT Acceptable Use Policy (AM-118-1) to ensure that the City's IT resources are used only in proper pursuit of the City's business; information is not improperly disclosed, modified or endangered; and access to the City's information resources is not made available to any unauthorized person.

A. The Chief Information Officer (CIO) is responsible for:

- Developing, implementing and communicating an IT strategic plan and the implementation roadmap for the City's IT strategic plan
- Monitoring the City's total IT spending and developing recommendations to optimize IT investments and equitable charge back to the Agencies
- Developing and maintaining the ITSM, security controls, standard operating procedures, and the standardization of IT Tools
- Implementing City-wide system change control procedures, communications, and IT training
- Providing input into the selection of Agency IT Directors and IT Leadership

- Providing end user support and guidance
- Developing usage, performance, IT metrics and service level agreements (SLAs)
- Developing and/or approving all customer facing applications, data and integration services
- Developing, maintaining and testing the City's IT Disaster Recovery Plan, Incident Response Plan, and IT Continuity of Operations (CoOp) Plan.
- Ensuring that all Agency IT procurements are aligned with the City's IT strategy, roadmap and standards
- Providing periodic updates on the City's compliance with IT Standards and recommendations for corrective actions to the Mayor's Office including the Mayor's Chief of Staff and Deputy Chief Administrative Officer, Agency Directors for DHR, Finance and Law and rotating Agency Operational Directors, as necessary.

B. The Chief Information Security Officer (CISO) is responsible for:

- Ensuring that appropriate security controls are in existence and practiced throughout the City
- Determining methods of implementing and enforcing IT Security Standards
- Advising IT resource owners and users on best practices to meet the City's IT Security Standards
- Maintaining the ITSM.

C. The Agency Head or designee bears responsibility for:

- Implementing the standards in the ITSM. Agencies may develop and implement Agency IT standards that exceed the City's IT Standards. In the case of conflicting standards, the stricter standard will apply
- Contacting BCIT prior to engaging with any vendors regarding the procurement of IT resources as defined in the Scope section of this policy to ensure the purchase is aligned with the City's IT Standards and meets our security requirements
- Adhering to BCIT Change Control Procedures anytime a change is made to an Agency supported production IT system
- Ensuring that all hardware and software is supported by the vendor. "Supported" means the vendor provides technical support in the event of a hardware or software failure and that the vendor provides regular software maintenance or patches to maintain performance and security. The Agency Head must execute an exception request for all unsupported hardware and software and commit to a timeline for removal or replacement.

Adherence to the IT Standards will be monitored and enforced using automated tools where feasible. The IT Standards will also be monitored and enforced through metrics, red / yellow / green scorecards and by IT audits or assessments.

IV. COMPLIANCE

Users found in violation of this Policy are subject to disciplinary action up to and including restriction, possible loss of privileges, suspension, or termination. If necessary, the City will notify the City's Law Department, OIG, or law enforcement of any legal violations.

V. RELATED POLICIES

AM 118-1 Technology Acceptable Use Policy