City of Milwaukee-

IT Security Plan

CONTENTS

OVERVIEW

The Information Security Plan as prepared by the Department of Administration - Information Technology Management Division (ITMD) provides a catalog of security policies to protect the confidentiality, integrity and availability of the City of Milwaukee's information. This document follows the recommended baseline security controls as outlined by The National Institute of Standards and Technology (NIST) in the NIST 800-53, R4 Special Publication for the protection of government systems.

NIST is a non-regulatory government agency that develops technology, metrics, and standards and provides guidance on recommended security controls for federal information systems. These standards have been widely adopted and are endorsed by the federal government because they encompass security best practices.

PURPOSE

The Information Security Plan was designed with the intention of providing managers, administrators, and other City employees with basic security strategies to be used in achieving an acceptable level of information security. Following NIST's cybersecurity framework, this plan establishes a guideline for the development and eventual implementation of a formalized City of Milwaukee Information Security Program to include Policies, Standards and Procedures. This plan will help the City to understand and communicate the importance of IT security and the security risks based on industry standards and best practices.

SCOPE

These policies apply to all City of Milwaukee data, systems, activities, and assets owned, leased, controlled, or used by City of Milwaukee personnel, its agents, contractors, or other business partners on behalf of the City of Milwaukee.

Some policies are explicitly stated for persons with a specific job function; unless otherwise noted, all personnel supporting the City of Milwaukee business functions shall comply with the policies. The City of Milwaukee departments or agencies shall use these policies or may create a more restrictive policy, but none that are less restrictive, less comprehensive, or less compliant than these policies.

These policies do not supersede any other applicable law or higher-level company directive, or existing labor management agreement as of the effective date of this policy.

Policies have been created to address each of the controls found in the NIST 800-53 V4 and are as follows:

AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS - Personnel Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

ROLES AND RESPONSIBILITIES

- Chief Information Officer (CIO)
  - Establishes the enterprise IT security plan
  - Reviews and proposes IT security policies to the City Information Management Committee (CIMC)
- Policy and Administration Manager, DOA/ITMD
  - Administers the DOA/ITMD IT security program
  - Formulates any DOA/ITMD-specific IT security standards
  - Provides guidance to the CIO for implementing and supporting IT federal, state, and local security laws and requirements
- Security and Audit Compliance Analyst DOA/ITMD
  - Researches and develops necessary IT security policies, standards, and procedures
  - Maintains the IT security policies, standards, and procedures review schedule
  - Publishes updates to the MINT policies section as necessary
  - Facilitates the processing of any requests for exceptions to security policies and standards
  - Provides IT security compliance consulting support as it relates to regulatory requirements and security industry best practices
  - Reports any concerns, trends or developments to the Policy and Administration Manager and CIO
- Information System Owner
  - Ensures that information systems are deployed, operated, maintained, and monitored according to agreed-upon security policies and procedures

COMPLIANCE

Realizing that the implementation of these policies will incur certain costs, managers should balance them against the potential costs associated with insufficient or nonexistent security practices. As a general rule, security-related costs are an integral part of information technology overhead.

The City's information security policies are dynamic and will be updated as required changes or additions are identified.

Compliance is to be enforced through current administrative procedures and is the responsibility of City managers and any appointed information security officers. Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

This document is a statement of City policy. For assistance in its interpretation and implementation, contact the CIO.

Instances of noncompliance and requests for exceptions to policy will be individually documented for review. The response may be the granting of an exception while accepting the user's plan or else proposing a different solution.

Requests for exceptions to policy shall be submitted by department managers to ITMD for review. Copies of each request and corresponding responses will be maintained in an exception to policy file. These records will remain on file as long as any situation of noncompliance exists even though an exception may have been granted.

COORDINATION AMONG AGENCIES

The City of Milwaukee is subject to multiple regulatory requirements designed to ensure the effective implementation of appropriate IT security measures. Listed below are the primary regulatory requirements:

- Centers for Medicare and Medicaid Services (CMS) - Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Criminal Justice Information Services (CJIS) Security Policy
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Social Security Administration (SSA) Technical System Security Requirements

It is the responsibility of each department and/or agency to safeguard assets and information including, but not limited to, Federal Tax Information (FTI), Protected Health Information (PHI), and Personally Identifiable Information (PII).

Note: All regulatory publications map to the security controls in NIST Special Publication 800-53, Revision 4, which is used as the primary reference point for IT security policies, standards, procedures.

IT SECURITY GOVERNANCE – TERMINOLOGY AND DEFINITIONS

The following definitions apply to this document:

- POLICIES
  - A policy is a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, rules, and objectives that must be met for a specific subject area.
  - Specific policies are created to mitigate risks within multiple categories that include, but are not limited to, information security, data privacy, and regulatory compliance.
- STANDARDS
  - A standard should make a policy more meaningful and effective. Standards are usually written to describe the requirements for various technology configurations (e.g., mobile devices, type in use for encryption, firewall settings).
  - A standard must include one or more accepted specifications for hardware, software, or behavior.
- PROCEDURES
  - Procedures are the specific instructions for aligning with standards and policies, consisting of a series of steps taken to accomplish an end-goal policy statement.
  - Procedures are important to achieving policy goals. The policies define what is to be protected. Procedures outline how to implement the standards or how to fulfill the requirements and expectations of the policies.
  - Regulatory requirements are defined to develop, document, and disseminate procedures to facilitate the implementation of associated policies.

ALIGNMENT WITH IT GOVERNANCE

Each department or agency shall be responsible for the management of the city's information security program at the department, or agency level. The CIO shall be responsible for the overall development, coordination, administration, and management of the program at the City-level and for establishing standards through which policy compliance will be measured.

COMMUNICATION

All approved security policies and standards will be published to MINT.

Policies, standards, and procedures will be communicated to all appropriate personnel upon approval.

IT security policies and standards will be incorporated into the City of Milwaukee's IT security awareness training program.

SECURITY POLICY AND STANDARDS REVIEW AND MAINTENANCE

The following processes will be implemented to ensure compliance to regulatory requirements.

IT security policies and standards will be reviewed annually or when changes to the information security environment occur. Revisions to the policy will be made to add clarity or resolve discrepancies between policies and standards.

The Security and Audit Compliance Analyst will:

- Document policy review and approval procedures
- Maintain the policy review schedule
- Publish IT security policies and standards to MINT
- Maintain a single repository for documentation that applies to all agencies
- Coordinate the review and tracking of exception requests to IT security policies and standards

NIST Reference: AC – Access Control	Implementation Date : June 6, 2019	Revision Number : 0.0

ACCESS CONTROL POLICY

PURPOSE

Access to City of Milwaukee's information technology assets shall be controlled and managed to ensure that only authorized devices/persons have appropriate access in accordance with business needs. The Access Control Policy is for managing risks associated with; user account management, access enforcement, monitoring, insufficient separation of duties, lack of adherence to the principle of least privilege, and remote access security.

SCOPE

All City of Milwaukee personnel responsible for approving and assigning access to the City's information systems are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Access Control Standard
  - AC-2 Account Management
  - AC-3 Access Enforcement
  - AC-5 Separation of Duties
  - AC-6 Least Privilege
  - AC-7 Unsuccessful Logon Attempts
  - AC-8 System Use Notification
  - AC-11 Session Lock
  - AC-12 Session Termination
  - AC-20 Use of External Information Systems
  - AC-21 Information Sharing
- Data Classification Standard
  - AC-22 Publicly Accessible Content
- Identification and Authentication Standard
  - AC-14 Permitted Actions without Identification or Authentication
- Remote Access Standard
  - AC-17 Remote Access
- Wireless Access Standard
  - AC-18 Wireless Access
- Mobile Device Standard
  - AC-19 Access Control for Mobile Devices

GENERAL POLICY

ACCOUNT MANAGEMENT

The City of Milwaukee utilizes automated system account management. Account creation and modifications will be completed after a formal request is received from an authorized requestor based on an approved business justification. Account management responsibilities are assigned to authorized account managers.

ACCOUNT ACCESS

Information system accounts shall be created, enabled, modified, disabled, and removed in accordance with City of Milwaukee defined procedures. Access is role based and granted on the principle of least privilege.

The City of Milwaukee has established safeguards against unauthorized access such as; password policies, acceptable use agreements, account lockouts after unsuccessful logon attempts, session idle timeouts, and session locks.

When an account poses, or has the potential to pose a significant risk, the account is either disabled and/or access attributes are removed. An account identifier is required to identify these accounts and prevent inappropriate re-enabling of account access. Re-enabling the account requires explicit approval of department management; self-service mechanisms may not be used to re-enable accounts.

All user accounts (including privileged) shall be disabled upon separation. In addition, credentials will be revoked in accordance with the Identification and Authentication Policy, and access attributes will be removed. Self-service mechanisms shall not be used to re-enable the account.Information sharing is restricted to authorized users based on access authorization and/or access restrictions dependent on the sensitivity of information to be shared. Access may be defined by group, organizational level, content type, or special access requests.

REMOTE ACCESS

Remote access to organizational information systems by users (or processes acting on behalf of users) through external networks will be authorized based on configuration/connection requirements and application guidance.

Automated monitoring and control of remote access sessions shall be implemented to protect the confidentiality and integrity of City data.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

SECURITY AWARENESS AND TRAINING POLICY

PURPOSE

This policy documents the security awareness and training requirements that each department or agency shall adhere to for the City of Milwaukee. All covered personnel are accountable for the accuracy, integrity, and confidentiality of the information to which they have access.

SCOPE

All new and existing employees, interns, consultants, and contractors, will complete security awareness training that informs them of information security policies, applicable procedures, and incident reporting, including insider threats. IT security awareness training shall include periodic briefings and continual reinforcement of best practices and standards in information security. Continual training may be accomplished using various types of technologies such as security bulletins, emails, and websites.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Security Awareness and Training Standard
  - AT-2 Security Awareness Training
  - AT-3 Role-Based Security Training
  - AT-4 Security Training Records

GENERAL POLICY

SECURITY AWARENESS TRAINING

Departments and agencies shall provide training relevant to effective information security practices to staff members in a timely manner. Training requirements include the following:

- Summary of information security policies, which shall be delivered by DOA/ITMD during orientation
- Information technology security training appropriate for work responsibilities, on a regular basis and whenever their work responsibilities change, (Managers shall delay covered personnel access to restricted or highly restricted data until initial training is complete.)
- Training on social engineering and how to detect it and respond to it
- Training on the acceptable use of City resources

SECURITY AWARENESS TRAINING – INSIDER THREAT

Insider threat training shall include how to communicate employee and management concerns and the prevention, detection, and response regarding potential indicators of insider threats through appropriate agency channels in accordance with established organizational policies and procedures.

Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices.

ROLE BASED SECURITY AWARENESS TRAINING

The extent of security related training shall reflect the person's individual responsibility for using, configuring, and/or maintaining information systems.

Role based security-related training shall be provided before authorizing a person's access to a system and before they are allowed to perform their assigned duties.

SECURITY TRAINING RECORDS

Individual security training activities, including basic security awareness training and information system specific security training, shall be monitored and documented.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: AU – Audit and Accountability	Implementation Date : June 6, 2019	Revision Number : 0.0

AUDIT AND ACCOUNTABILITY POLICY

PURPOSE

The purpose of the Audit and Accountability Policy is to enforce the City of Milwaukee's commitment to protect information and critical resources by providing a plan to respond to incidents and minimize the impact to City assets. The Audit and Accountability Policy is for managing risks from inadequate event logging and transaction monitoring. The related audit and accountability standards and procedures ensure the implementation of security best practices regarding event logging and transaction monitoring and the retention of audit evidence.

The audit and log functions shall enable the detection and capture of event data of unauthorized access to sensitive and classified information, and information requiring regulatory protection. Audited events shall be reviewed regularly and where possible when unauthorized access events have been identified.

Auditing shall be enabled to the greatest extent necessary to capture; access, modification, deletion, and movement of sensitive and classified information by unique user name/ID. Event storage retention shall remain in compliance with regulatory requirements and be supported with an appropriate amount of disk storage for the required retention period. Time-stamp capabilities shall be synchronized for monitoring auditable devices and events.

SCOPE

Information system owners in charge of monitoring of information systems and supporting infrastructure are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Audit and Accountability Standard
  - AU-2 Audit Events
  - AU-3 Content of Audit Records
  - AU-4 Audit Storage Capacity
  - AU-5 Response to Audit Processing Failures
  - AU-6 Audit Review, Analysis, and Reporting
  - AU-8 Time Stamps
  - AU-9 Protection of Audit Information
  - AU-11 Audit Record Retention
  - AU-12 Audit Generation

GENERAL POLICY

AUDIT EVENTS

An audit event is any observable occurrence in an agency's information system that is significant and relevant to the security of information systems and the environments in which those systems operate. System owners shall detect these events and protect the integrity and availability of information systems by monitoring operational audit logs.

The City of Milwaukee information system owners shall establish a current, reliable baseline that can be compared to audit logs to determine whether any abnormalities are present.

Logs shall be reviewed and updated annually or when a major change to the information system occurs. Over time, the events that shall be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

CONTENT OF AUDIT RECORDS

Information systems shall be configured to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event

AUDIT STORAGE CAPACITY

Audit record storage capacity shall be sufficient to retain audit records for the required audit retention period. This is to provide support for after-the-fact investigations of security incidents and to meet regulatory and state information retention schedule requirements.

RESPONSE TO AUDIT PROCESSING FAILURES

Alerts will be configured to notify defined personnel in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

AUDIT REVIEW, ANALYSIS, AND REPORTING

In order to protect the integrity and availability of the City of Milwaukee's data, operational audit logs will be monitored and reviewed.

Designated staff will regularly review system, application and user event logs, for abnormalities. Any discovered abnormalities and/or discrepancies between the logs and the baseline shall be reported to department management.

Access to audit logs shall be restricted to only those authorized to view them and the logs shall be protected from unauthorized modifications.

System audit records shall be reviewed weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized access.

AUDIT REDUCTION AND REPORT GENERATION

Audit reduction and report generation capability shall be implemented to support on-demand audit review, analysis, and reporting requirements following security incidents

TIME STAMPS

Internal system clocks shall be used to generate time stamps for audit records that are mapped to either Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) or local time with an offset from UTC that meets a defined time synchronization and source.

PROTECTION OF AUDIT INFORMATION

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion by utilizing protection controls. Authorized access to audit functionality will be limited to a defined subset of privileged users.

AUDIT RECORD RETENTION

Audit records shall be retained and disposed of in accordance with the City's retention schedules.

AUDIT GENERATION

DOA/ITMD will provide audit record generation capability for defined auditable events pertaining to network, server, and user environments.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

City of Milwaukee

Security Assessment and Authorization Policy

NIST Reference: CA – Security Assessment and Authorization	Implementation Date : June 6, 2019	Revision Number : 0.0

SECURITY ASSESSMENT AND AUTHORIZATION POLICY

PURPOSE

The Security Assessment and Authorization Policy and the associated procedures help to implement security best practices regarding security assessments, authorization, and continuous monitoring.

SCOPE

Individuals performing designated roles in the security assessment and authorization process are responsible that processes are executed and maintained in compliance with City policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Security Assessment and Authorization Standard
  - CA-2 Security Assessments
  - CA-3 System Interconnections
  - CA-5 Plan of Action and Milestones
  - CA-7 Continuous Monitoring
  - CA-8 Penetration Testing

GENERAL POLICY

SECURITY ASSESSMENTS

The City of Milwaukee will develop a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements
- Assessment procedures to be used to determine security control effectiveness
- The assessment environment, team, and roles and responsibilities

SYSTEM INTERCONNECTIONS

The City of Milwaukee authorizes connections from information systems to other information systems with the use of interconnection agreements. These agreements will document for each interconnection; the interface characteristics, security requirements, and nature of the information communicated. The security agreements will be reviewed and updated as necessary.

PLAN OF ACTION AND MILESTONES

A plan of action will be developed to address weaknesses or vulnerabilities identified during an assessment exercise. Updates to the plan of actions will be based on findings from security control assessments, impact analysis, and continuous monitoring.

CONTINUOUS MONITORING

A continuous monitoring strategy will be implemented to facilitate ongoing awareness of threats and vulnerabilities to the City's information systems. The strategy will include:

- Establishment of metrics and frequency of assessment monitoring
- Development of response plans to address vulnerabilities
- Reporting structure

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: CM – Configuration Management	Implementation Date : June 6, 2019	Revision Number : 0.0

CONFIGURATION MANAGEMENT POLICY

PURPOSE

The Configuration Management Policy is for managing risks from system changes affecting baseline configuration settings, system configuration, and security. The configuration management procedures will help document, authorize, manage, and control system changes affecting information system components.

To ensure a secured and consistent implementation of protection mechanisms, baseline configurations and supporting procedures for all City applications shall be developed, documented, and maintained. These baselines shall follow best practices, e.g., those outlined by CIS (Center for Internet Security) benchmarks or the United States Government Configuration Baseline (USGCB). Regulatory requirements shall be reviewed at least annually and updates made to agency system environments as needed.

SCOPE

All personnel involved in configuration, risk and change management of information systems and supporting infrastructure are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Configuration Management Standard
  - CM-2 Baseline Configuration
  - CM-3 Configuration Change Control
  - CM-4 Security Impact Analysis
  - CM-6 Configuration Settings
  - CM-7 Least Functionality
  - CM-8 Information System Component Inventory

GENERAL POLICY

BASELINE CONFIGURATIONS/INFORMATION SYSTEM COMPONENT INVENTORY

The City of Milwaukee information system owners will develop and maintain baseline documentation of current information systems. Baseline documentation will consist of; information system design, information system architecture, configuration settings and associated documentation.

CONFIGURATION CHANGE CONTROL

Standard changes shall be formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation.

CONFIGURATION SETTINGS

Configuration management procedures will be developed to document the processes to support secure system development life cycle activities at the information system level. Baseline secure and compliant configurations must be reviewed and updated at a minimum of annually or as required due to system upgrades, patches, or other significant changes.

LEAST FUNCTIONALITY

Information systems will be configured to provide only essential capabilities, specifically disabling, prohibiting, or restricting the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: CP – Contingency Planning	Implementation Date : June 6, 2019	Revision Number : 0.0

CONTINGENCY PLANNING POLICY

PURPOSE

To ensure continuation of operations, the Contingency Planning Policy is for managing risks from information asset disruptions, failures, and disasters through the establishment of effective contingency planning procedures. The contingency planning procedures ensure the implementation of security best practices regarding business continuity and disaster recovery plans.

SCOPE

DOA/ITMD shall be responsible for developing, maintaining, testing, and communicating the City of Milwaukee's contingency plan. All essential systems will be identified and documented within a formal contingency plan, along with procedures that define recovery objectives, restoration priorities, success metrics that include recovery time and recovery point objectives, roles and responsibilities, and contact lists. The contingency plan shall be reviewed on an annual basis.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Contingency Planning Standard NIST 800 53
  - CP-2 Contingency Plan
  - CP-3 Contingency Training
  - CP-4 Contingency Plan Testing
  - CP-6 Alternate Storage Site
  - CP-8 Telecommunications Services
  - CP-9 Information System Backup
  - CP-10 Information System Recovery

GENERAL POLICY

CONTINGENCY PLAN INFORMATION, PROCEDURES TO INCLUDE:

- Computer Emergency Communications Plan: Who is to be contacted, when, and how? What immediate actions shall be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance
- The order of recovery in both short-term and long-term timeframes

- Data Backup and Restoration: Provide detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It shall also describe how that data could be recovered.
- Equipment Replacement: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Crisis Communication Structure: Who is responsible for communication?
- Crisis Communication Templates for DOA/ITMD staff and the City of Milwaukee call center.

CONTINGENCY PLAN MANAGEMENT

- The plan shall be distributed to key personnel and organizational elements.
- The plan shall be reviewed, and updated annually.
- Testing of the Contingency Plan shall be performed annually to include an alternate storage, processing, and telecommunications site

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: IA – Identification and Authentication	Implementation Date : June 6, 2019	Revision Number : 0.0

IDENTIFICATION AND AUTHENTICATION POLICY

PURPOSE

The Identification and Authentication Policy establishes the City of Milwaukee's plan for managing risks from user access (organizational, non-organizational) and authentication into information assets through the establishment of an effective identification and authentication program.

SCOPE

All authorized City of Milwaukee personnel responsible for identity authentication and role definition, are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

ACCESS CONTROL STANDARD

- Identification and Authentication Standard
  - IA-2 Identification and Authentication (Organizational Users)
  - IA-3 Device Identification and Authentication
  - IA-4 Identifier Management
  - IA-5 Authenticator Management
  - IA-6 Authenticator Feedback
  - IA-7 Cryptographic Module Authentication
  - IA-8 Identification and Authentication (Non-Organizational Users)

GENERAL POLICY

IDENTIFICATION AND AUTHENTICATION

To ensure the security and integrity of The City of Milwaukee's data, all users (or processes acting on behalf of users) will be uniquely identified and authenticated prior to accessing the City's information systems.

AUTHENTICATOR MANAGEMENT

On an annual basis, designated Information Security Officers and department managers shall review user account documentation for compliance. These reviews shall be conducted on a system wide basis. Reviews will examine:

- Levels of access
- Conformity with the concept of least privilege
- Appropriate documentation and authorizations are secured

AUTHENTICATOR FEEDBACK

Feedback of authentication information is obscured during authentication processes to protect the information from possible exploitation and use by unauthorized individuals. Obscuring the feedback of authentication information includes for example, displaying asterisks when users type passwords into input devices.

CRYPTOGRAPHIC MODULE AUTHENTICATION

All information systems shall implement approved mechanisms for authentication to a cryptographic module, which meet applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for authentication.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: IR – Incident Response	Implementation Date : June 6, 2019	Revision Number : 0.0

INCIDENT RESPONSE POLICY

PURPOSE

The purpose of the Incident Response Policy is to increase the availability of City resources, to rapidly detect incidents, minimize any loss due to destruction, mitigate weaknesses that were exploited, and restore computing services.

SCOPE

All City of Milwaukee personnel involved with the identification, response, reporting, assessment, analysis, and follow-up to all suspected information security incidents involving information systems and supporting infrastructure are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Incident Response Standard NIST 800-53
  - IR-2 Incident Response Training
  - IR-3 Incident Response Testing
  - IR-4 Incident Handling
  - IR-5 Incident Monitoring
  - IR-6 Incident Reporting
  - IR-8 Incident Response Plan

GENERAL POLICY

INCIDENT RESPONSE TRAINING

Departments shall provide training to information system users consistent with assigned roles and responsibilities before authorizing access to information systems.

INCIDENT RESPONSE TESTING

Incident handling for security incidents will include procedures for preparation, detection and analysis, containment, eradication and recovery in a finalized Incident Response Plan (IRP). DOA/ITMD will test the incident response capability for the City of Milwaukee annually using checklists, walk-throughs, tabletop exercises, simulations or other such methods as deemed necessary to determine the incident response effectiveness. Incident response procedures will be reviewed and revised accordingly to include lessons learned following ongoing incident handling activities.

INCIDENT RESPONSE HANDLING, MONITORING, REPORTING

City of Milwaukee departments and agencies shall designate information security monitoring roles to individuals with the responsibility of monitoring, analyzing, and reporting security alerts. Security alerts will be distributed to appropriate personnel. Automated alerts for intrusion detection, intrusion prevention, and file integrity monitoring systems will also be in place. The Incident response reporting structure is outlined in the City of Milwaukee's Contingency Plan.

INCIDENT RESPONSE PLAN

An incident response plan will be in place to provide a roadmap for implementing an incident response strategy. The incident response plan will define reportable incidents, identify metrics for measuring risks and priorities, establish crisis communication standards, and provide steps to be taken to effectively manage and mature the City of Milwaukee's incident response capability.

The incident response plan will be reviewed and approved annually and revised as needed in response to system changes or issues encountered during plan implementation, execution or testing.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: MA – Maintenance	Implementation Date : June 6, 2019	Revision Number : 0.0

MAINTENANCE POLICY

PURPOSE

The System Maintenance Policy addresses the information security aspects of information system maintenance and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity.

SCOPE

All authorized City of Milwaukee personnel involved in the maintenance of information systems and supporting infrastructure are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- System Maintenance Standard
  - MA-2 Controlled Maintenance
  - MA-3 Maintenance Tools
  - MA-4 Non-Local Maintenance
  - MA-5 Maintenance Personnel

GENERAL POLICY

CONTROLLED MAINTENANCE

Designated City of Milwaukee personnel shall:

- Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements
- Approve, monitor, and document maintenance activities to the City of Milwaukee's information system or system components. This includes both on and off-site maintenance
- Require that remote maintenance and use of diagnostic tools will be restricted to approved methods as outlined in the remote access security procedures

MAINTENANCE TOOLS

Maintenance tools used specifically for diagnostic and repair actions will be approved controlled and monitored by information system owners.

MAINTENANCE PERSONNEL

The City of Milwaukee shall:

- Establish a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel
- Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations
- Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations

- REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: MP – Media Protection	Implementation Date : June 6, 2019	Revision Number : 0.0

MEDIA PROTECTION POLICY

PURPOSE

The Media Protection Policy is for managing risks from media access, media storage, and media transport through the establishment of effective media protection procedures. Media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, mobile devices including portable storage media such as USB memory sticks and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, tablets, smartphones and cellular telephones, digital cameras, and audio recording devices and non-digital media (e.g., paper, microfilm).

SCOPE

All City of Milwaukee personnel involved in the handling of media are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Media Protection NIST 800-53
  - MP-2 Media Access
  - MP-4 Media Storage
  - MP-5 Media Transport
  - MP-6 Media Sanitization

GENERAL POLICY

MEDIA ACCESS

Access to all digital and non-digital media is restricted to authorized individuals only, using pre-defined security measures. Departments and agencies at their discretion may restrict the use of removable media in environments that process highly restricted data.

Access controls shall include physical protection of and accountability for removable media to minimize the risk of damage and/or unauthorized access to data stored on the removable storage media.

MEDIA STORAGE

Media protection is required during the life cycle of the storage medium until such time the media has been physically destroyed or sanitized using only approved destruction equipment, techniques, and procedures. Stored data shall be protected and backed up so that restoration can occur in the event of accidental or unauthorized deletion or misuse.

MEDIA TRANSPORT

Protection mechanisms should be implemented to protect sensitive or regulated information whether at rest or in transit.

MEDIA SANITIZATION

Media content shall be destroyed or sanitized, based on classification, prior to removal of the media device from any secured location/facility to an unauthorized individual(s) or location/facility. The following media sanitization requirements are required:

- Media sanitization or destruction shall be witnessed or verified. If sanitization is not possible, the media device will be destroyed in a way that renders the media not readable and unrecoverable.
- The technique for clearing, purging, and destroying media depends on the type of media being sanitized. Media sanitization requirements are the same, regardless of where the information system media is located.
- Review, approve, track, document, and verify media sanitization and disposal actions

- REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

City of Milwaukee

Physical and Environmental Protection Policy

NIST Reference: PE – Physical and Environmental Protection	Implementation Date : June 6, 2019	Revision Number : 0.0

PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY

PURPOSE

The Physical and Environmental Protection Policy is for mitigating the risks to the City of Milwaukee's datacenters from physical security and environmental threats through the establishment of effective physical security and environmental control procedures.

Physical access to facilities where sensitive and/or confidential informational assets or infrastructure resides will be strictly. All personnel granted access to restricted buildings should display appropriate identification badges.

SCOPE

As the provider of the City's data center, DPW shall protect environmental control equipment (HVAC), monitoring systems and required power cabling, control boxes, and piping from inappropriate access, tampering, damage and destruction. Further protection of the infrastructure components shall include emergency shutoff, power, lighting, fire protection (detection and suppression), temperature and humidity controls, and water damage protection.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Physical and Environment Protection Standard
  - PE-2 Physical Access Authorizations
  - PE-3 Physical Access Control
  - PE-4 Access Control for Transmission
  - PE-6 Monitoring Physical Access
  - PE-8 Visitor Access Records
  - PE-9 Power Equipment and Cabling
  - PE-10 Emergency Shutoff
  - PE-11 Emergency Power
  - PE-12 Emergency Lighting
  - PE-13 Fire Protection
  - PE-14 Temperature and Humidity Controls
  - PE-15 Water Damage Protection

GENERAL POLICY

PHYSICAL AND ENVIRONMENTAL PROTECTION PROCEDURES

All City of Milwaukee facilities are required to coordinate and implement necessary procedures for providing physical and environmental protection and preventing unauthorized access to IT resources and information systems. Periodic reviews of this policy shall be performed and documented at least annually, or when there is a significant change.

PHYSICAL ACCESS AUTHORIZATIONS AND CONTROL

Departments will develop, approve and maintain a list of individuals with authorized access to the facility or designated area where information systems reside. Authorization credentials (e.g., badges, identification cards, and smart cards) must be issued. The level of access provided to each individual must not exceed the level of access required to complete the individual's job responsibilities. A periodic physical access review is conducted at least annually.

ACCESS CONTROL FOR TRANSMISSION MEDIUM

Physical access to information system distribution and transmission lines within organizational facilities shall be controlled.

Protective measures must include the following:

- Locked wiring closets
- Disconnected or locked spare jacks
- Protection of cabling by conduit or cable trays

MONITORING PHYSICAL ACCESS

Physical access to information system locations will be monitored to detect and respond to physical security incidents. Physical access logs are reviewed monthly. Physical intrusion alarms and surveillance equipment are monitored, and investigations performed if necessary for apparent security violations, suspicious physical access, etc. •

VISITOR CONTROL

Visitor access records to the facility where the information system resides will be maintained and reviewed at least annually.

Location of information system components are positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

POWER EQUIPMENT AND CABLING

The City of Milwaukee, DPW will protect power equipment and power cabling for information systems from damage and destruction.

EMERGENCY SHUTOFF

DPW provides the capability of shutting off power to the information system or individual system components in emergencies. Emergency shutoff switches or devices will be placed in secure locations to facilitate safe and easy access for personnel while protecting emergency power shutoff capability from unauthorized activation.

EMERGENCY POWER/LIGHTING

Short-term uninterruptible power supplies will be provided to facilitate an orderly shutdown of critical information systems in the event of a primary power source loss.

Emergency lighting shall be provided for information systems, which will activate in the event of a power outage or disruption.

PROTECTION CONTROLS

Protection devices and controls for fire, temperature and water where critical information systems are located, will be maintained and monitored by DPW.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: PL – Security Planning	Implementation Date : June 6, 2019	Revision Number : 0.0

SECURITY PLANNING POLICY

PURPOSE

The Security Planning Policy is for managing risks from inadequate security through the establishment of an effective security-planning program. The related security planning standards and procedures ensure the implementation of best practices.

SCOPE

All City of Milwaukee personnel are responsible for adhering to this policy. If a department or agency identifies security issues that may require modification to the security plan, the agency has the responsibility to consult with DOA/ITMD.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Planning
  - PL 2 System Security Plan
  - PL-4-Rules of Behavior

GENERAL POLICY

SYSTEM SECURITY PLAN

DOA/ITMD shall develop, distribute, review, and update annually, the Information Security Plan. The plan will address purpose, scope, roles and responsibilities, management commitment and coordination among City departments and agencies.

RULES OF BEHAVIOR

Rules describing responsibilities and expected behavior concerning information and information systems will be made readily available to individuals requiring access to the information system.

Role based security training will be provided by authorized individuals before access is granted to information system resources.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: PS – Personnel Security	Implementation Date : June 6, 2019	Revision Number : 0.0

PERSONNEL SECURITY POLICY

PURPOSE

The Personnel Security Policy is for managing risks from personnel screening, termination, management, and third party (contractors, vendors, interns) access, through the establishment of effective security planning procedures.

SCOPE

All City of Milwaukee personnel responsible for authorizing individual access to information systems are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Personnel Security Standard
  - PS-4 Personnel Termination
  - PS-5 Personnel Transfer
  - PS-6 Access Agreements

GENERAL POLICY

PERSONNEL TERMINATION

Upon notice of termination, an individual's information system access will be disabled. Information systems and related property will be retrieved. Access to organizational information and information systems formerly controlled by a terminated individual will be retained.

PERSONNEL TRANSFER

When an individual from the City of Milwaukee transfers to another position or department, operational access will be reviewed, confirmed, and modified according to operational needs for authorization to information systems/facilities.

ACCESS AGREEMENTS

Access agreements for the City of Milwaukee information systems will be developed and documented. Access agreements shall be reviewed and updated as necessary.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: RA – Risk Assessment	Implementation Date : June 6, 2019	Revision Number : 0.0

RISK REVIEW POLICY

PURPOSE

The Risk Review Policy is established so that the impact of an information system compromise can be reduced in an efficient manner. The related risk assessment procedures will ensure the implementation of security best practices in response to the identification of known vulnerabilities to the City of Milwaukee information systems.

Timely risk assessments of business functions, information assets, and systems are required to protect against potential threats and vulnerabilities in the areas of confidentiality, integrity, and availability of sensitive and confidential information. Assessments consist of steps to:

- Determine business requirements and potential business impacts from compromise
- Identify the impact that could occur from an information system compromise
- Determine areas of vulnerabilities
- Identify threats and the likelihood of compromise
- Initiate appropriate remediation activities to remediate or mitigate vulnerabilities and threats

SCOPE

All authorized City of Milwaukee personnel involved in risk management of information systems and supporting infrastructure are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Risk Assessment Standard
  - RA-3 Risk Assessment
  - RA-5 Vulnerability Scanning

GENERAL POLICY

RISK ASSESSMENT

System owners will assess risk, 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.

The risk assessment results will be documented, reviewed, and updated annually or whenever there are significant changes to the information systems environment.

Risk assessment results should be included in the City's Contingency Plan.

VULNERABILITY SCANNING

Vulnerability scanning of information systems and hosted applications shall be performed monthly or when new vulnerabilities are identified or reported.

Vulnerability scanning tools and techniques that promote interoperability among tools and that automate parts of the vulnerability management process will be used to:

- categorize platforms, software flaws and improper configurations
- develop checklists and test procedures
- analyze, remediate and document vulnerability reports

- REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: SA – System and Services Acquisition	Implementation Date : June 6, 2019	Revision Number : 0.0

SYSTEM AND SERVICES ACQUISTION POLICY

PURPOSE

The System (assets) and Services Acquisition policy provides documentation of the minimum requirements for IT security considerations before, during, and after the IT procurement process.

SCOPE

All City of Milwaukee personnel involved in the acquisition, development, or operation of information systems and supporting infrastructure are responsible for adhering to this policy and with any local system and service acquisition requirements.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- System and Services Acquisition Standard
  - SA-2 Allocation of Resources
  - SA-3 System Development Life Cycle
  - SA-4 Acquisition Process
  - SA-5 Information System Documentation
  - SA-8 Security Engineering Principles
  - SA-9 External Information System Services
  - SA-10 Developer Configuration Management
  - SA-11 Developer Security Testing and Evaluation

GENERAL POLICY

ALLOCATION OF RESOURCES

City of Milwaukee departments, and/or agencies shall work with DOA/ITMD to determine information security requirement before purchasing information systems or applications new to the environment. Any required security resources shall be included in the budgeted amount.

SYSTEM DEVELOPMENT LIFE CYCLE

Product or service life cycle methodologies used by the vendor must include security controls that address information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions.

ACQUISITION PROCESS

The following requirements, descriptions, and criteria, shall be included in the contract for the acquisition of information systems, system components, or information system services in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

- Security functional requirements
- Security strength requirements
- Security assurance requirements
- Security-related documentation requirements
- Requirements for protecting security-related documentation
- Description of the information system development environment and environment in which the system is intended to operate
- Acceptance criteria

INFORMATION SYSTEM DOCUMENTATION

Information system owners will obtain system administrator and user documentation for the information system, system component, or information system service

System administrator documentation to include:

- Secure configuration, installation, and operation of the system component or service
- Effective use and maintenance of security functions/mechanisms
- Known vulnerabilities regarding configuration and use of administrative functions

User documentation to include:

- User-accessible security functions/mechanisms and use
- Methods for user interaction, which enables individuals to use the system, component or service in a more secure manner
- User responsibilities in maintaining security requirements
- Document protection
- Document availability to department defined personnel or roles

SECURITY ENGINEERING PRINCIPLES

Information system security engineering principles shall be applied in the specification, design, development, implementation, and modification of the organizations information systems.

EXTERNAL INFORMATION SYSTEM SERVICES

Providers of external organizational information system services shall comply with information security requirements and employ security controls in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, and guidelines.

DEVELOPER CONFIGURATION MANAGEMENT

Developers of the City's information systems shall be required to:

- Perform configuration management during development, implementation and operation of the organizations information systems, system components or system services
- Document, manage and control the integrity of changes to configuration items
- Implement only department approved changes to the organizations systems
- Document approved changes and potential security impacts of changes
- Track security flaws and flaw resolution

DEVELOPER SECURITY TESTING AND EVALUATION

Security testing and evaluation of the City's information systems should include:

- The creation and implementation of a security assessment plan
- System testing/evaluation
- Documentation of security assessments
- Flaw remediation process

- REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

City of Milwaukee

System and Communication Protection Policy

NIST Reference: SC – System and Communication Protection	Implementation Date : June 6, 2019	Revision Number : 0.0

SYSTEM AND COMMUNICATION PROTECTION POLICY

PURPOSE

The System and Communications Protection Policy is for managing risks from vulnerable system configurations, denial of service, data communication, and transfer. The associated system and communications protection procedures help implement security best practices as they relate to the availability, confidentiality, or integrity of information.

Sensitive and confidential agency information, whether at rest or in-transit, shall be protected from accidental or intentional threats that could corrupt, modify, delete, or disclose that information.

SCOPE

All authorized City of Milwaukee personnel involved in risk management of data communication are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROL RECOMMENDATIONS THAT WILL BE INCLUDED IN THE FINAL POLICY

- System and Communications Protection Standard
  - SC-4 Information in Shared Resources
  - SC-5 Denial of Service Protection
  - SC-7 Boundary Protection
  - SC-8 Transmission Confidentiality and Integrity
  - SC-10 Network Disconnect
  - SC-12 Cryptographic Key Establishment and Management
  - SC-13 Cryptographic Protection
  - SC-19 Voice Over Internet Protocol
  - SC-20 Secure Name/Address Resolution Service (Authorative Source)
  - SC-23 Session Authenticity
  - SC-28 Protection of Information at Rest

GENERAL POLICY

INFORMATION IN SHARED RESOURCES

Unauthorized and unintended information transfer via shared system resources shall be prevented in accordance with the Access Control and Identification and Authentication policies when system processing explicitly switches between different users, information classification levels, or security categories.

DENIAL OF SERVICE PROTECTION

The effects of denial of service (DoS) or distributed denial of service (DDoS) attacks shall be limited by appropriately securing all hosts that could be potential targets.

BOUNDARY PROTECTION

Communications shall be controlled and monitored at the external boundary of the system and at key internal boundaries within the system. Connections to external networks or information assets through managed interfaces shall consist of boundary protection devices arranged in accordance with City of Milwaukee security architecture standards.

TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Transmitted information shall be protected to ensure that the confidentiality and integrity of the data are maintained during the transfer process.

Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure of information and/or to detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

NETWORK DISCONNECT

Remote access will be configured to disconnect inactive sessions.

CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

DOA/ITMD shall establish and manage cryptographic keys for required cryptography employed within the information systems in accordance with ITMD's defined requirements for key generation, distribution, storage, access, and destruction. Recovery procedures must be tested at least annually to ensure agency access and availability to encrypted data.

CRYPTOGRAPHIC PROTECTION

The City of Milwaukee shall implement cryptographic modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

VOICE OVER INTERNET PROTOCOL

Usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies will be established based on the potential to cause damage to the information system if used maliciously.

SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORATIVE SOURCE)

Data origin authentication and data integrity verification will be performed on the name/address resolution responses the system receives from authoritative sources using recursive resolving or caching domain name system (DNS) servers.

SESSION AUTHENTICITY

The information system must protect the communications sessions. Protection mechanisms shall be selected and implemented to protect data integrity, confidentiality, and session authenticity in transmission.

PROTECTION OF INFORMATION AT REST

The City of Milwaukee shall protect the confidentiality and integrity of all Restricted or Highly Restricted data at rest.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: SI – System and Information Integrity	Implementation Date : June 6, 2019	Revision Number : 0.0

SYSTEM AND INFORMATION INTEGRITY POLICY

PURPOSE

The System and Information Integrity Policy is for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling. The related system and information integrity procedures help the City of Milwaukee implement best practices regarding system configuration, security, and error handling.

SCOPE

All City of Milwaukee personnel involved in the acquisition, development, or operation of information systems and supporting infrastructure are responsible for adhering to this policy and with any local system and service acquisition requirements.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS PATCH MANAGEMENT STANDARD

- System and Information Integrity Standard
  - SI-2 Flaw Remediation
  - SI-3 Malicious Code Protection
  - SI-4 Information System Monitoring
  - SI-8 Spam Protection

GENERAL POLICY

FLAW REMEDIATION

Information system flaws will be identified, reported, and corrected. This includes any potential vulnerabilities resulting from those flaws. Software and firmware updates to address system flaws will be tested before installation. Security software and firmware updates shall be installed within 30 days of release.

MALICIOUS CODE PROTECTION

The City of Milwaukee will employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. Malicious code protection will be updated whenever a new release is available.

Malicious code protection mechanisms will be configured to perform periodic scans of the information

INFORMATION SYSTEM MONITORING

The integrity of sensitive and regulated information shall be maintained and be protected against compromise by potential threats and vulnerabilities. All critical security event mechanisms shall have event detection monitoring, capturing, and reporting of violation events.

Security violation event records will be logged and retained based on current applicable regulatory requirements.

SPAM PROTECTION

The City of Milwaukee shall employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages. Spam protection shall be updated when new releases are available in accordance with the configuration management policies and procedures.

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created
June 2019	DOA/ITMD	Final Draft Completed

NIST Reference: PM – Program Management	Implementation Date : June 6, 2019	Revision Number : 0.0

PROGRAM MANAGEMENT POLICY

PURPOSE

The Program Management Policy sets specifications for the development, assessment, authorization, and monitoring of the IT security program. The successful implementation of security controls for organizational systems depends on the successful implementation of the organization's program management controls.

The Information Security Program was developed in response to the requirements outlined by the following:

- Wisconsin Statutes Chapter 16 assigns responsibility of proper privacy and security procedures/safeguards; information security planning; threat-mitigation, and resource development to the Department of Administration.
- NIST SP 800-53 Revision 4, which defines baseline security controls for governmental organizations, requires identification and documentation of the senior-level official(s) responsible for information security programs.

SCOPE

All City of Milwaukee personnel involved in the development, delivery, and implementation of the City's Information Security Program Management are responsible for adhering to this policy.

STANDARDS AND ASSOCIATED NIST SECURITY CONTROLS

- Program Management Standard
  - AC-1 Access Control
  - AT-1 Awareness and Training
  - AU-1 Audit and Accountability
  - CA-1 Security Assessment and Authorization
  - CM-1 Configuration Management
  - CP-1 Contingency Planning
  - IA-1 Identification and Authentication
  - IR-1 Incident Response
  - MA-1 Maintenance
  - MP-1 Media Protection
  - PL-1 Planning
  - PS-1 Personnel Security
  - RA-1 Risk Assessment
  - SA-1 System and Services Acquisition
  - SC-1 System and Communication Protection

- SI-1 System and Information Integrity
- PM-1 Program Management

GENERAL POLICY

ASSIGNED INFORMATION SECURITY RESPONSIBILITIES AND BUSINESS PROCESS

- Structure of the City's Information Security Program Management:
  - The CIO proposes the IT security policies and standards to the City Council and Mayor for adoption. Once adopted, the security policies and standards will provide a baseline to be used throughout the City of Milwaukee. DOA/ITMD will be responsible for publishing and maintaining these documents.
  - As needed to address business requirements, City departments and agencies can employ more rigorous policies and standards in relation to agency-specific applications and processes.
- IT security policies and standards will be reviewed at least annually
- The CIO is the designated official assigned with the responsibility to create an information security program, securing resources (including assistance from internal and external personnel and IT assets) to coordinate, develop, implement, and maintain the information security program

REVISION HISTORY

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed

APPENDIX A – ACRONYMS

COMMON IT SECURITY ABBREVIATIONS ADOPTED FROM NIST SPECIAL PUBLICATION 800-37, REVISION 4

- APT Advanced Persistent Threat
- CIO Chief Information Officer
- CISO Chief Information Security Officer
- CJIS Criminal Justice Information Services
- CPO Chief Privacy Officer
- DOA Department of Administration
- DNS Domain Name System
- DOA Department of Administration
- DoD Department of Defense
- FAR Federal Acquisition Regulation
- FEA Federal Enterprise Architecture
- FERPA Family Educational Rights and Privacy Act
- FICAM Federal Identity, Credential, and Access Management
- FIPS Federal Information Processing Standards
- FISMA Federal Information Security Management Act
- HIPAA Health Insurance Portability and Accountability Act
- HSPD Homeland Security Presidential Directive
- IPsec Internet Protocol Security
- IRS Internal Revenue Service
- LACS Logical Access Control System
- NIST National Institute of Standards and Technology
- NSA National Security Agency
- OMB Office of Management and Budget
- OPSEC Operations Security
- PCI-DSS Payment Card Industry Data Security Standard
- PII Personally Identifiable Information
- PIV Personal Identity Verification
- PKI Public Key Infrastructure
- RMF Risk Management Framework
- SCADA Supervisory Control and Data Acquisition
- SP Special Publication
- TCP/IP Transmission Control Protocol/Internet Protocol
- USB Universal Serial Bus
- USGCB United City Government Configuration Baseline
- VoIP Voice over Internet Protocol
- VPN Virtual Private Network

APPENDIX B – GLOSSARY/DEFINITIONS

Term	Definition
Access Control	Security control designed to permit authorized access to an IT system or application.
Accessible	Information arranged, identified, indexed, or maintained in a manner that permits the custodian of the public record to locate and retrieve the information in a readable format within a reasonable time.
Authentication	Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Availability	The extent to which information is operational, accessible, functional, and usable upon demand by an authorized entity (e.g., a system or user)
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Configuration Management	The process of keeping track of changes to the system, if needed, approving them.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Response	The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual
Information Asset	Information and systems that provide value to an agency or organization
Integrity	Integrity is the protection of information from tampering, forgery, or accidental changes. It ensures that messages are accurately received as they were sent, and computer errors or non-authorized individuals do not alter information.

Term	Definition
Least Functionality	The organization configures information systems to provide only essential capabilities, and disables unused or unnecessary components of information systems to prevent unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.
Least Privilege	Granting users, programs, or processes only the access they specifically need to perform their business task and no more.
Multifactor Authentication	Using more than one of the following factors to authenticate to a system: Something you know (e.g., user-ID, password, personal identification number (PIN), or passcode); something you have (e.g., a one-time password authentication token, 'smart card'); something you are (e.g., fingerprint, retina scan).
Privileged Account	A privileged account is an account, which provides increased access and requires additional authorization. Examples include a network, system, or security administrator account.
Remote Access	The connection of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information.
Risk	The probability that a particular threat will exploit a particular vulnerability of the system.
Risk Assessment	The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.
Security (IT)	Measures and controls that protect IT systems/information against denial of access and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions.
Social Engineering	Social engineering is a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites.
System	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and communications.
Threat	A potential circumstance, entity, or event capable of exploiting vulnerability and causing harm. Threats can come from natural causes, human actions,

Term	Definition
	or environmental conditions. A threat does not present a risk when there is no vulnerability.
User	Any State Entity, federal government entity, political subdivision, their employees or third-party contractors or business associates, or any other individuals who are authorized by such entities to access a system for a legitimate government purpose.
Vulnerability	A weakness that can be accidentally triggered or intentionally exploited.

Appendix C – Review, Revision, Approval Log

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	06/24/2019	Draft IT Security Policy Plan	Judy Siettmann	