NIST Reference: AC – Access Control	Implementation Date : June 6, 2019	Revision Number : 2.0

Access Control Policy

Purpose

The Access Control Policy establishes a framework for controlling access to information and information systems by ensuring that only authorized personnel have access to the City's valuable assets and resources. The policy aims to protect the confidentiality, integrity, and availability of information by defining access control requirements and procedures that are based on business needs, risk management principles, and regulatory compliance requirements. By implementing effective access controls, the policy enhances the City's information security posture and reduces the risk of unauthorized access, modification, or disclosure of sensitive information

Scope

This policy applies to all employees, contractors, and authorized personnel who access, use, or manage the City's information systems, applications, and data. It covers all information systems owned or operated by the City, whether they are located on-site or accessed remotely.

Roles and Responsibilities

Management

Management is responsible for establishing and enforcing account management policies and procedures, allocating necessary resources, and ensuring compliance with relevant regulations and standards.

System Administrators

System administrators are responsible for implementing and maintaining automated account management systems, performing account provisioning and revocation, and monitoring account activities.

Information Security

Information Security is responsible for overseeing account management practices, conducting periodic audits, and ensuring compliance with the City of Milwaukee's access control policies.

Users

Users are responsible for adhering to account management procedures, safeguarding their account credentials, and reporting any suspected security incidents or unauthorized account activities.

NIST security controls

AC-1 Policy and Procedure

This document is intended to serve as the Access Control Policy and is made available to applicable personnel. To facilitate the implementation of the Access Control Policy and associated physical and environmental protection controls, the City shall develop, document, and disseminate the corresponding procedure(s) to all relevant individuals.

AC-2 Account Management

Account management within the City of Milwaukee's information systems shall follow established procedures for creating, enabling, modifying, disabling, and removing information system accounts.

AC-2(1) Account Management | Automated System Account Management

The City of Milwaukee shall establish streamlined workflows, define roles and responsibilities, and develop detailed procedures for the account provisioning process, utilizing an Identity and Access Management (IAM) system. Roles and responsibilities shall be clearly defined to ensure accountability and compliance with policies and security requirements. Procedures shall be developed, providing guidelines for user identification, authentication, and authorization during the account provisioning process.

A self-service portal shall be implemented, allowing users to change their passwords. The self-service portal will include clear instructions, and password complexity requirements to ensure secure password modifications.

AC-2(3) Account Management | Disable Accounts

Upon notification to ITMD, active directory accounts of terminated employees shall be disabled immediately. It is crucial for this action to occur promptly, preferably during or before termination. If confidentiality is required prior to termination, the department may contact the CIO or the ITMD Policy and Admin Manager. In cases where a department needs to maintain an email account for a separated employee, a written request should be submitted to the CIO, providing a reason, and specifying the duration for which the account should remain active. Such accounts shall not remain active for more than 90 days. For vacancies of elected officials, the duration for which the account remains open will be determined on a case-by-case basis.

AC-2(5) Account Management | Inactivity Logout

Screensaver lockouts are essential for maintaining information security and safeguarding sensitive data. These lockouts automatically activate after a period of user inactivity, requiring users to reauthenticate through password or other authentication mechanisms to regain access to their devices. By implementing screensaver lockouts, we prevent unauthorized access to unattended workstations, minimizing the risk of data breaches and unauthorized use of resources. Screensaver lockouts serve as an effective deterrent against insider threats and unauthorized access attempts, ensuring that only authorized personnel can access and interact with our systems and data. This measure reinforces our commitment to protecting the confidentiality, integrity, and availability of critical information, promoting a secure computing environment for the City of Milwaukee and its stakeholders.

Session lock shall be implemented to prevent unauthorized access to devices when the currently signed-in user leaves without locking the desktop. The Active Directory security policy setting "Interactive Logon: Machine inactivity limit" will be configured to 15 minutes (900 seconds). If the inactive time exceeds this limit, the user's session will lock by invoking the screen saver. Screen savers are activated on destination machines, requiring password authentication. Exceptions to this setting will be determined based on high availability requirements.

AC-2(13) Account Management | Disable Accounts for High-risk Individuals

Accounts belonging to high-risk individuals, such as terminated employees, individuals involved in security incidents, or those with compromised credentials, shall be disabled immediately upon request from authorized individuals.

AC-3 Access Enforcement

Information system accounts will be created, enabled, modified, disabled, and removed in accordance with the defined procedures of the City of Milwaukee. Access will be role-based and granted based on the principle of least privilege. A listing of authorized users in these roles must be documented and maintained. Each role may belong to one or more individuals depending on the application. User accounts should be reviewed annually.

The City of Milwaukee will implement safeguards against unauthorized access, such as password policies, acceptable use agreements, account lockouts after unsuccessful logon attempts, session idle timeouts, and session locks. Accounts that pose or have the potential to pose a significant risk will be disabled and/or have their access attributes removed. Account re-enabling will require explicit approval from department management, and self-service mechanisms cannot be used for this purpose.

All user accounts, including privileged accounts, will be disabled upon separation. 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 will be restricted to authorized users based on access authorization and/or access restrictions depending on the sensitivity of the information to be shared. Access may be defined by group, organizational level, content type, or special access *requests.*

Individual Accounts

1. User accounts will be created after a request is received by authorized departmental personnel following the standard naming convention.
2. User account permissions and level of system access are assigned based upon an individual's role.
3. If an individual has several departmental roles, with conflicting levels of access, the most restrictive policy applies.
4. Upon creation or reset of an account, the system should prompt the user to create an initial password that complies with the Password Complexity Standard. In cases where this is not possible, the initial password must be unique, comply with the Password Complexity Standard, and require that the user change the password upon the first use.

Privileged Accounts

1. A privileged account is an account that provides increased access and requires additional authorization. Examples include a network, system, or security administrator account. The use of privileged accounts must be compliant with the principle of least privilege. Access will be restricted to only those programs or processes specifically needed to perform authorized business tasks and no more.
2. Authorized individuals with privileged access, such as account administrators, will be issued additional accounts. Privileged access will not be assigned to standard user accounts.
3. The passwords to system and service accounts essential to the operation of an information system must be known or accessible to more than a single person. Such passwords must meet complexity requirements, be stored in a secure manner, and changed on a schedule relative to the risk of exposure or at a minimum when those with knowledge of the password terminate or are reassigned.
4. To provide audit visibility into privileged accounts, systems must be designed and configured to log events linked to privileged accounts. All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs, including third-party vendors, must be securely logged, and reviewed monthly in accordance with the Audit and Accountability Standard.

Access Control Restrictions:

Access to sensitive data must be restricted to authorized personnel based on their job roles and responsibilities. Downloading sensitive data to personal accounts or devices is strictly prohibited, unless explicit authorization is granted by the CIO.

AC-4 Information Flow Enforcement

Information flow control mechanisms shall be implemented to prevent unauthorized or inappropriate dissemination of sensitive information. Data loss prevention (DLP) solutions, encryption, digital rights management (DRM), and other appropriate technologies shall be utilized to control information flow and prevent data leakage. Information classification and labeling shall be implemented to clearly identify the sensitivity level of data and guide its appropriate handling and distribution.

AC-5 Separation of Duties

Separation of duties shall be implemented as a security control principle to prevent conflicts of interest, reduce the risk of errors and fraud, and enhance compartmentalization. It shall involve dividing critical tasks and responsibilities among different individuals or roles to ensure that no single person shall have complete control over a process or system.

AC-6 Least Privilege

The City of Milwaukee adheres to the principle of least privilege, granting only the minimum necessary system privileges required to perform their job duties. The following measures have been put in place to ensure compliance with the least privilege requirements:

1. To access a designated list of security functions and pertinent security information, individuals must obtain explicit authorization through the account authorization process.

2. Individuals with access to information system accounts, roles, or other security functions are required to use a unique, non-privileged account for non-administrative functions.

3. Privileged accounts on the information system are restricted to predefined personnel or roles.

4. Regular audits of information systems are conducted to review privileged function execution.

5. Non-privileged users are prevented from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards or countermeasures.

AC-7 Unsuccessful Logon Attempts

To ensure user account security and prevent unauthorized access, the City of Milwaukee shall implement measures to monitor and address unsuccessful login attempts. Security controls and systems shall track and analyze failed login attempts, identifying potential malicious activities or unauthorized access attempts. When a predefined threshold of unsuccessful login attempts is reached, appropriate actions should be taken, such as temporary account lockout, investigation initiation, or alert triggering to the IT security team.

AC-8 System Use Notification

The City of Milwaukee's information systems shall display a system use notification when users access the system. This notification remains on the screen until users explicitly acknowledge and take action to log on or further access the system.

AC-11 Device Lock

The City of Milwaukee's information systems shall have session locks that activate after no more than fifteen (15) minutes of inactivity or upon user request. The session lock remains in effect until the user re-establishes access using their login credentials.

AC-14 Permitted Actions without Identification or Authentication

In specific situations within the City of Milwaukee's information systems, limited circumstances may allow certain actions to be performed without the need for identification or authentication. These

exceptions shall be strictly controlled, monitored, and documented to ensure they do not compromise system security.

AC-17 Remote Access

Users granted remote access privileges shall be subject to the City of Milwaukee's identification and authentication policies and procedures. Access shall be authorized based on documented business needs and approved by appropriate management. Remote access shall be restricted to authorized users with a legitimate business need. User access rights and privileges shall be aligned with the principle of least privilege, granting only the necessary access required to perform authorized tasks. Remote access shall be granted for a defined period and reviewed periodically to ensure ongoing business need and appropriateness.

All remote access connections shall be encrypted using strong cryptographic protocols and algorithms to protect the confidentiality and integrity of transmitted data. Network segmentation and firewalls shall be implemented to separate remote access networks from internal networks, limiting potential attack vectors and unauthorized access attempts. Remote access sessions shall be logged and monitored to detect and respond to any security incidents or unauthorized activities promptly. Mobile devices used for remote access shall adhere to the City of Milwaukee's Mobile Device Management (MDM) policies and security controls, including encryption, device authentication, and remote wipe capabilities.

AC-18 Wireless Access

Wireless access points and networks shall be implemented to ensure secure and authorized wireless access. Authentication mechanisms, such as strong passwords, certificate-based authentication, or other approved methods, shall be enforced to verify the identity of wireless users and devices.

Wireless networks shall be periodically scanned and assessed for vulnerabilities and unauthorized access points to maintain a secure wireless environment. By adhering to these requirements, the City of Milwaukee ensures a robust and secure wireless access infrastructure, protecting sensitive data and mitigating the risk of unauthorized access.

AC-19 Access Control for Mobile Devices

Mobile devices shall be protected with strong access controls to prevent unauthorized access and safeguard sensitive information. Access to mobile devices shall be controlled through user authentication mechanisms, such as passwords, PINs, biometrics, or other approved authentication methods, as specified in the City of Milwaukee's Identification and Authentication Standard. Full device or container-based encryption shall be enforced on all mobile devices to protect the confidentiality and integrity of data stored on these devices.

Mobile devices shall be regularly patched and updated with the latest security patches and firmware releases to address known vulnerabilities. Mobile devices shall be protected by up-to-date anti-malware software to detect and mitigate potential threats. Lost or stolen mobile devices shall be reported immediately to the appropriate IT personnel or helpdesk to initiate appropriate response actions, such as remote wipe or lock.

Mobile devices shall be configured with appropriate network security controls, such as virtual private network (VPN) connectivity, to establish secure connections when accessing City of Milwaukee's information systems remotely. Mobile devices shall be protected by physical security measures, such as device lock mechanisms or secure storage, to prevent unauthorized access.

AC-20 Use of External Systems

The City of Milwaukee has established terms and conditions to allow authorized access to City resources from external information systems, as applicable. Additional terms and conditions shall be implemented to authorize individuals to process, store, and/or transmit City-controlled information using these external information systems.

The City of Milwaukee permits the use of external information systems for accessing its systems or processing, storing, and transmitting information, provided that the required security measures are implemented and verified on the external system. This compliance is in accordance with the City of Milwaukee's information security policy and security plan.

The use of City-controlled portable storage devices by authorized individuals on external information systems is strictly prohibited.

AC-21 Information Sharing

To facilitate information sharing, the City of Milwaukee shall enable authorized users to verify whether access authorizations assigned to sharing partners align with the access restrictions on the information. This is particularly important in defined information sharing circumstances that require user discretion. Additionally, defined automated mechanisms or manual processes shall be employed to assist users in making informed decisions regarding information sharing and collaboration.

AC-22 Publicly Accessible Content

Only designated and authorized individuals shall be granted the privilege to post information onto the City of Milwaukee’s information system for public access. These authorized individuals shall undergo specific training to ensure that publicly accessible information does not contain any non-public information, safeguarding the confidentiality of sensitive data.

All content published as publicly accessible must adhere to these legal requirements, including the protection of intellectual property rights, copyright laws, and other applicable regulations. Moreover, non-public information, such as personally identifiable information (PII) and sensitive data, shall not be included in publicly accessible content unless explicitly authorized and in compliance with privacy regulations.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

Assessment, Authorization, and Monitoring Policy

NIST Reference:	Implementation Date :	Revision Number :
CA – Assessment, Authorization and Monitoring	June 2019	2.0

Assessments, Authorization and Monitoring Policy

Purpose

The Assessment, Authorization and Monitoring Policy establishes a framework for conducting regular assessments to evaluate the effectiveness of controls, aiming to identify vulnerabilities and areas for improvement. By promptly addressing any deficiencies, the policy enhances the City's information security posture and protects its valuable assets and resources.

Scope

This policy applies to all systems, networks, and assets within the City of Milwaukee that are subject to control assessments. It encompasses all personnel involved in the assessment process, including management, independent assessors, and relevant stakeholders.

Roles and Responsibilities

Management

Management holds the responsibility of approving and enforcing the Control Assessments Policy. They allocate the necessary resources for conducting control assessments, designate individuals to oversee the assessment process, and authorize control assessments. Management reviews and acts upon assessment reports and findings to ensure effective control implementation.

Information Security

Information Security is responsible for developing and maintaining the Control Assessments Policy and associated procedures. They coordinate and facilitate the control assessment process, providing guidance and support to independent assessors. The Information Security Team ensures the secure exchange of assessment-related information and maintains records of control assessment authorizations and findings.

System Administrators

System Administrators collaborate on control assessments and provide necessary access to systems and assets. They implement recommended control enhancements and remediation actions, monitor the effectiveness of controls, and promptly report any deviations or incidents.

NIST security controls

CA-1 Policy and Procedures

The City of Milwaukee shall establish and maintain a comprehensive policy and accompanying procedures for conducting control assessments. These findings will be documented, communicated, and made readily accessible to all relevant personnel within the City.

CA-2 Control Assessments

Control assessments shall be conducted periodically within the City of Milwaukee to evaluate the effectiveness and efficiency of information security controls. These assessments will cover the design, implementation, and operational aspects of controls, ensuring a thorough evaluation of the City's information security posture.

CA-2(1) Control Assessments | Independent Assessors

To ensure objectivity and impartiality, the City will engage independent assessors to perform control assessments. Criteria and qualifications for independent assessors will be defined by the City, and their results and findings will be considered in control assessment reports.

CA-3 Information Exchange

The City will establish mechanisms for secure information exchange related to control assessments. These mechanisms will facilitate internal information sharing and, when necessary, enable the City to exchange relevant information with external stakeholders, in compliance with applicable privacy and confidentiality requirements.

CA-5 Plan of Action and Milestones

Control assessment findings and identified vulnerabilities will be documented and tracked using a structured Plan of Action and Milestones (POA&M) process. The POA&M will include corrective actions, responsible parties, and target completion dates, enabling the City to effectively manage and remediate identified issues.

CA-6 Authorization

Control assessments within the City will be authorized by appropriate management or designated authorities. This authorization process will ensure that control assessments are conducted consistently and systematically, while also maintaining appropriate accountability. Records of control assessment authorizations will be maintained.

CA-7 Continuous Monitoring

Continuous monitoring activities will be performed within the City to assess the ongoing effectiveness of information security controls. The City will establish procedures for collecting, analyzing, and reporting monitoring data to identify potential control deficiencies and trigger necessary corrective actions.

CA 7(4) Continuous Monitoring | Risk Monitoring

Risk monitoring will be integrated into the City's continuous monitoring process to identify and assess changes in risk exposure. The City will establish mechanisms for detecting and responding to significant changes in risk levels. Risk monitoring activities will consider internal system connections and their potential impact on overall risk.

CA 9 Internal System Connections

The City will identify and document internal system connections to assess their impact on information security. Control assessments will consider the security requirements and controls associated with these internal system connections. Regular reviews and updates of the documentation will be conducted to ensure its accuracy and relevance.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Audit and Accountability Policy**

NIST Reference:	Implementation Date :	Revision Number :
AU – Audit and Accountability	June 6, 2019	2.0

Audit and Accountability Policy

Purpose

The Audit and Accountability Policy plays a crucial role in upholding the City of Milwaukee's commitment to safeguarding information and critical resources. Its primary objective is to establish a comprehensive plan that effectively addresses incidents and minimizes the impact on City assets. This policy specifically focuses on managing risks associated with insufficient event logging and transaction monitoring.

Scope

This policy is applicable to all information systems, applications, and data within the City's infrastructure. It covers all employees, contractors, and authorized personnel who access, use, or manage City information systems. The policy applies to both on-site and remote systems and encompasses all system components involved in the processing, storage, or transmission of City data.

Roles and Responsibilities

Management

Management plays a crucial role in the implementation of the Audit and Accountability Policy within the City of Milwaukee. Their responsibilities include developing and approving the policy, allocating necessary resources, monitoring compliance, and acting based on audit findings. They provide guidance and oversight, ensuring the policy's effectiveness and addressing any identified issues. Management sets the tone for accountability and emphasizes the importance of protecting information and critical resources.

Information Security

Information Security is responsible for overseeing audit and compliance functions related to the organization's information security, ensuring adherence to policies, regulations, and industry best practices.

System Administrators

The IT department collaborates with Information Security to implement technical controls and solutions necessary for effective event logging, transaction monitoring, and auditing. They are responsible for configuring and maintaining systems that capture and retain relevant audit data.

NIST security controls

AU-1 Policy and Procedures

The City of Milwaukee is dedicated to upholding a secure information environment. To achieve this goal, we have established an Audit Logging Policy to ensure the comprehensive and accurate recording of events in our information systems. By implementing and adhering to this policy, our aim is to enhance our ability to identify and mitigate risks, protect sensitive information, and ensure compliance with applicable regulations and standards.

AU-2 Event Logging

Audit records play a crucial role in supporting security monitoring, forensic analysis, and compliance assessments. To ensure their effectiveness, information systems shall be configured to generate and retain comprehensive and accurate audit records. These records shall contain relevant details, including event type, timestamp, location, source, outcome, and associated individuals or subjects. By serving as a reliable audit trail, these records facilitate the detection, investigation, and response to security incidents, bolstering the overall security posture of the organization.

AU-3 Content of Audit Records

All audit records generated by the City of Milwaukee systems shall contain the following content:

1. Event Type: Each record shall clearly indicate the type of event or activity that occurred, providing insight into the nature of the event, such as logins, file access, system changes, or security incidents.

2. Timestamp: The records shall include precise timestamps, capturing the date and time of each event, enabling proper sequencing and chronological analysis of system activities.

3. Source and Destination Addresses: Audit records shall document the source and destination addresses associated with network-based events, facilitating the identification and analysis of network traffic patterns.

4. User Identification: Each record shall include user identification information, such as usernames or unique identifiers, to attribute specific actions to individual users, ensuring accountability and aiding in investigations.

5. Object or Resource Accessed: Audit records shall identify the specific objects or resources involved in each event, such as files, databases, or system components, providing contextual information for incident response and forensics.

6. Outcome of the Event: The records shall indicate the outcome of each event, including whether it was successful, unsuccessful, or resulted in an error or exception, assisting in the identification of potential security incidents or system anomalies.

AU-4 Audit Log Storage Capacity

The City of Milwaukee shall maintain an appropriate audit storage infrastructure that meets the following criteria:

1. Sufficient Capacity: The storage system shall provide adequate capacity to accommodate the expected volume of audit records generated by the information systems, considering factors such as the organization's size, data retention requirements, and anticipated growth.

2. Scalability: The audit storage solution shall be scalable to accommodate future increases in the volume of audit records without compromising performance or accessibility.

3. Retention Period: Audit records shall be retained for the duration specified by applicable regulations, and state information retention policy requirements. The storage system shall support the defined retention period, and procedures shall be established to ensure timely deletion or archiving of expired records.

AU-5 Response to Audit Logging Process Failures

In support of the City's commitment to a secure environment, the following actions will be taken in the event of an auditing process failure:

1. Identification and Notification: Prompt identification of any failures or anomalies in the audit logging process is crucial. Once detected, responsible personnel shall be immediately notified to initiate the response process.

2. Investigation and Root Cause Analysis: Upon notification, a thorough investigation shall be conducted to determine the root cause of the audit logging process failure. This includes examining system logs, analyzing configurations, and interviewing relevant personnel.

3. Mitigation and Resolution: Appropriate measures shall be taken to mitigate the impact of the failure and restore the proper functioning of the audit logging process. This may involve troubleshooting, applying patches or updates, adjusting configurations, or seeking support from relevant vendors or technical experts.

4. Documentation and Reporting: All audit logging process failures, their root causes, and the actions taken to resolve them shall be documented. This information shall be reported to the relevant stakeholders, including management, the Information Security Officer, and any applicable audit committees or regulatory bodies.

5. Lessons Learned and Process Improvement: An analysis of the audit logging process failure shall be conducted to identify any lessons learned and opportunities for process improvement. Recommendations shall be made to enhance the effectiveness and resilience of the audit logging process, and necessary adjustments shall be implemented.

AU-6 Audit Record Review, Analysis, and Reporting

The following procedures shall be followed for audit record review, analysis, and reporting:

1. Regular Review: Audit records shall be reviewed on a scheduled basis to ensure compliance with organizational policies, regulatory requirements, and industry best practices. This includes the examination of relevant event types, timestamps, source information, and user activities.

2. Event Correlation and Analysis: Audit records shall be analyzed for patterns, trends, and potential indicators of security incidents or vulnerabilities. Event correlation techniques, such as cross-referencing multiple audit records or utilizing security information and event management (SIEM) systems, may be employed to identify complex or subtle threats.

3. Incident Response and Investigation: In the event of suspected security incidents or anomalies, audit records shall be thoroughly investigated to gather evidence and support incident response efforts. This includes tracing the sequence of events, identifying the root causes, and capturing relevant forensic information.

4. Reporting and Documentation: Findings from audit record reviews, analyses, and investigations shall be documented and reported to the appropriate stakeholders. This includes management, the Information Security Officer, incident response teams, and any relevant regulatory or compliance entities, as required.

5. Continuous Improvement: Based on the outcomes of the review, analysis, and reporting processes, necessary adjustments and improvements to the audit logging and monitoring practices shall be identified and implemented. This ensures the ongoing effectiveness and efficiency of the audit record review process.

AU-8 Time Stamps

The City shall maintain a Time Stamps policy to ensure accurate and consistent time synchronization across information systems. Internal clocks should be configured to synchronize with a reliable time source and Coordinated Universal Time (UTC) shall be used for time stamps in audit records.

AU-9 Protection of Audit Information

To maintain the confidentiality and integrity of audit information, strict access controls will be implemented, limiting access to authorized personnel. User access privileges will adhere to the principle of least privilege, ensuring individuals have access only to the audit information relevant to their roles and responsibilities. Additionally, audit information will be encrypted at rest and in transit to safeguard it against unauthorized access, disclosure, or manipulation.

Storage systems utilized for storing audit information will be secure and resilient, with regular backups conducted to ensure data integrity and availability.

AU-11 Audit Record Retention

To comply with regulatory and organizational information retention requirements, audit records shall be retained in accordance with the Records Retention and Disposition Schedules. The purpose of retaining these records is to support after-the-fact investigations of security incidents and ensure adherence to relevant regulations. By maintaining proper retention of audit records, the City can effectively analyze and review historical events, mitigate potential risks, and demonstrate compliance with retention policies and legal obligations.

AU-12 Audit Record Generation

To ensure consistency and accuracy, audit records shall be automatically generated by information systems without manual intervention. This automated process minimizes errors and ensures a reliable audit trail. Audit records shall be generated in a timely manner to capture events as close to real-time as possible.

Information systems responsible for generating audit records shall be properly configured and regularly tested to ensure adherence to policy requirements.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Awareness and Training Policy**

NIST Reference:	Implementation Date :	Revision Number :
AT –Awareness and Training	June 6, 2019	2.0

Awareness and Training Policy

Purpose

The Awareness and Training Policy establishes the requirements for each department or agency within the City of Milwaukee. It emphasizes the accountability of covered personnel for maintaining the accuracy, integrity, and confidentiality of the information they access.

Scope

All employees, interns, consultants, and contractors, whether new or existing, are required to complete security awareness training. This training will provide them with an understanding of information security policies, relevant procedures, and incident reporting protocols, including insider threats. IT security awareness training will include regular briefings and continuous reinforcement of best practices and standards in information security. Various technologies, such as security bulletins, emails, and websites, may be utilized to deliver ongoing training.

Roles and Responsibilities

Management

Management plays a critical role in promoting a culture of security awareness and driving the implementation of security training programs. They allocate resources and provide support to ensure the successful rollout of these initiatives. Additionally, leaders set the example by actively participating in security training, emphasizing the importance of security, and championing a proactive approach to mitigating security risks.

Information Security

Information Security is responsible for designing, developing, and delivering comprehensive security training programs .They collaborate with relevant stakeholders to identify training needs, develop engaging content, and ensure that the training materials align with the city's security policies and procedures. Information Security stays abreast of emerging threats and industry best practices, ensuring

that the training remains current and relevant. They also assess the effectiveness of the training programs and make necessary improvements to enhance their impact.

Department Managers and Supervisors

Department managers and supervisors play a crucial role in supporting security training initiatives within their respective departments. They ensure that employees within their teams receive the required security training and actively participate in the programs. Department managers and supervisors reinforce the importance of security awareness, encourage employees to apply the knowledge gained from training in their daily work, and provide guidance and support to address security concerns. By fostering a culture of security within their departments, they contribute to creating a vigilant and security-conscious workforce.

NIST security Controls

AT-1 Policy and Procedures

This document is intended to serve as the Security Awareness and Training Policy and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the Security Awareness and Training Policy and related physical and environmental protection controls shall be developed, documented, and disseminated to all applicable personnel.

AT-2 Literacy Training and Awareness

All personnel shall participate in literacy training programs to enhance their general security knowledge and understanding. The City of Milwaukee shall provide training modules that cover common security terminology, concepts, and best practices. Regular assessments and evaluations shall be conducted to measure the effectiveness of literacy training initiatives. By ensuring the participation of all personnel in these programs, the city aims to establish a solid foundation of security literacy throughout the workforce, enabling employees to make informed decisions and contribute to a strong security posture.

AT-2(2) Literacy Training and Awareness | Insider Threat

In order to mitigate the risks associated with insider threats, all personnel shall receive insider threat training. This training shall encompass education on how to effectively communicate concerns related to employees and management, as well as the prevention, detection, and response to potential indicators of insider threats. Such communication shall be conducted through appropriate agency channels, adhering to established policies and procedures. Potential indicators and precursors of insider threat, including long-term job dissatisfaction, attempts to access unauthorized information, unexplained access to financial resources, bullying or harassment of fellow employees, workplace violence, and serious violations of city policies, shall be highlighted and addressed during the training.

AT-2(3) Literacy Training and Awareness | Social Engineering and Mining

To enhance awareness and mitigate the risks associated with social engineering and data mining, all personnel shall undergo specialized training. The training programs shall provide comprehensive modules, equipping employees with knowledge of the techniques utilized in social engineering attacks and the potential consequences of data mining activities. Personnel shall be trained to identify and

appropriately respond to social engineering attempts, such as phishing, SMS phishing, and baiting, in order to safeguard sensitive information from unauthorized access or manipulation.

AT-3 Role Based Training

Training programs shall be tailored to meet the specific security responsibilities and knowledge requirements of different roles. This ensures that personnel receive training aligned with their job functions, equipping them with the necessary skills to effectively fulfill their security obligations. Role-based training shall cover a range of topics, including secure coding practices, data handling procedures, incident response protocols, and compliance requirements. By providing targeted training based on individual roles, the city aims to enhance security awareness and enable employees to apply their training directly to their respective job responsibilities.

AT-4 Training Records

Accurate and up-to-date training records shall be maintained for all personnel. These records will include essential details such as training dates, topics covered, attendance records, and assessment results. To ensure the integrity and confidentiality of these records, they shall be securely stored. The proper maintenance of training records enables the city to demonstrate compliance with training requirements, monitor employee progress, and identify areas for improvement. These records serve as a valuable resource for ensuring accountability and evaluating the effectiveness of the training programs.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Removed ITMD from orientation.
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Configuration Management Policy**

NIST Reference:	Implementation Date :	Revision Number :
CM – Configuration Management	June 6, 2019	2.0

Configuration Management Policy

Purpose

The Configuration Management Policy is designed to effectively manage risks associated with system changes that impact baseline configuration settings, system configuration, and security. It aims to ensure the integrity and security of information systems by implementing systematic and controlled processes for managing configuration changes.

Scope

The scope of the configuration management policy encompasses the management and control of all configuration items (CIs) within the City's IT infrastructure. This includes hardware, software, and network devices as defined as critical assets in the City of Milwaukee Contingency Plan. The primary objective of configuration management is to establish and maintain the integrity, consistency, and accuracy of configuration data throughout the entire lifecycle of IT assets. All personnel involved in configuration, risk, and change management of information systems and supporting infrastructure are responsible for adhering to this policy.

Roles and Responsibilities

Management

Management is responsible for ensuring the effective implementation of this security policy. They will provide the necessary resources, support, and oversight to enable proper configuration management practices and compliance with this policy.

System Administrators

System administrators are responsible for implementing and maintaining the configuration management procedures outlined in this policy. They will ensure that systems are configured securely,

changes are properly authorized and documented, and the system component inventory is accurate and up to date.

NIST security controls

CM-1 Policy and Procedures

The City of Milwaukee shall establish and implement comprehensive policy and procedures for configuration management. This policy shall be documented and communicated to relevant personnel or roles within the organization. It will address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements.

CM-2 Baseline Configuration

A Baseline Configuration refers to a formally reviewed and agreed-upon set of specifications for a system or Configuration Item (CI) within a system at a specific point in time. It can only be modified through change control procedures. The baseline configuration serves as the foundation for future builds, releases, and changes.

For each information system, including its associated components, an approved baseline configuration that aligns with operational requirements and constraints shall be developed, reviewed, approved, documented, and maintained under configuration control. The responsibility for baseline configurations lies with the Information Technology Management Department.

The baseline configuration documentation must include the following information about the components of an information system:

- Standard operating system and installed applications with current version numbers
- Standard software load for workstations, servers, network components, and mobile devices and laptops
- Up-to-date patch level information
- Network topology
- Logical placement of the component within the system and enterprise architecture

As the information system evolves over time, new baselines must be created to ensure the maintenance of an up-to-date baseline configuration. Previous versions of baseline configurations should be retained to support rollbacks when necessary.

CM-3 Configuration Change Control

Change Control outlines the process of managing updates to baseline configurations. Configuration change control for information systems involves the systematic proposal, justification, implementation, test/evaluation, review and documentation of changes.

Access restrictions shall be defined, approved, and documented to enforce configuration control processes. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Configuration change control is the process for ensuring that configuration changes to an information system are formally requested, evaluated for their security impact, tested for effectiveness, and approved before they are implemented.

Configuration Change Control Process:

- Plan – Identify the Change
- Analyze – Determine the Impact and Risk
- Approval – Moderate and High Risks require approval from CIO.
- Test – Changes will be tested in development or test environments.
- Implement – Test and verify in production.
- Close – Evaluate and document.

CM-4 Impact Analysis

Configuration changes shall be evaluated and documented to assess their potential impact on the security and functionality of the information system.

Routine or Standard Changes:

Routine or standard changes are defined as low-risk, well-defined changes that are frequently performed and have minimal impact on the system or organization. These changes follow established procedures or templates and have minimal disruption to the system or organization. Routine changes are pre-approved by designated authorities or change managers, and their implementation follows documented procedures.

Minor Changes

Minor changes, as defined by this policy, are relatively low-risk modifications with a limited impact on the system or organization. They encompass minor enhancements, updates, or fixes that can be managed without extensive scrutiny or high-level approvals. Minor changes require approval from designated authorities based on documented guidelines and must adhere to the established change management processes.

Major Changes

Major changes are substantial modifications with a higher level of risk, complexity, or impact on the system or organization. These changes involve careful planning, coordination, and evaluation, such as significant system upgrades, infrastructure overhauls, or new technology introductions. Approval for major changes is obtained through evaluation by relevant stakeholders, technical experts, or change review boards. The approval is granted by designated authorities based on the assessed risks and impacts. Detailed testing and implementation plans are required to ensure the proper execution of major changes.

Emergency Changes

In exceptional circumstances, emergency changes may be necessary. Emergency changes are unplanned and urgent modifications aimed at addressing critical issues or mitigating risks. These changes are implemented under exceptional circumstances and require immediate approval from designated

authorities or emergency change review boards. Post-implementation, emergency changes are documented and reviewed.

CM-5 Access Restrictions for Changes

Access to modify system configurations shall be limited to authorized personnel. To ensure proper control and documentation, change management procedures shall be implemented. Only individuals with the required privileges and approvals shall be granted access to make changes to configurations.

CM-6 Configuration Settings

Configuration management procedures shall be developed and implemented to establish and maintain baseline secure and compliant configurations for all information systems. These procedures shall specify the security settings, parameters, and controls necessary to ensure the integrity, confidentiality, and availability of the systems. Baseline configurations shall be reviewed and updated at least annually or as required due to system upgrades, patches, or other significant changes.

CM-7 Least Functionality

Information systems shall be configured to provide only essential capabilities required for system or application functionality. Unnecessary or unused system services, ports, network protocols, and capabilities shall be disabled, prohibited, or restricted to minimize the attack surface and reduce the risk of unauthorized access or exploitation.

CM-8 System Component Inventory

The City of Milwaukee shall maintain an accurate and up-to-date inventory of all system components, encompassing hardware, software, and network devices. Configuration management procedures shall incorporate clear processes for identifying, documenting, and managing system components throughout their lifecycle. The inventory shall encompass essential details, including component type, version, location, and relevant security controls.

CM-10 Software Usage Restrictions

The City of Milwaukee shall establish procedures to enforce software usage restrictions on information systems. Only authorized and licensed software shall be installed and utilized on the systems. Software installations and updates shall adhere to approved change management processes and undergo monitoring to verify compliance with licensing agreements and City policies.

CM-11 User Installed Software

Users will not be allowed to install unauthorized software on organization-owned systems. Configuration management procedures shall include measures to prevent the installation of unapproved software and regular monitoring to detect and remove any unauthorized software. Authorized software installations shall be performed by designated personnel following established change management processes.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security

needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Contingency Planning Policy**

NIST Reference:	Implementation Date :	Revision Number :
CP – Contingency Planning	June 6, 2019	2.0

Contingency Planning Policy

Purpose

The Contingency Planning Policy establishes a comprehensive framework for business continuity and contingency planning within the City of Milwaukee. It aims to ensure the continued operation and resilience of critical business functions, assets, and systems in the face of disruptions or disasters.

Scope

Contingency planning involves the development and implementation of strategies, procedures, and measures to enable the effective response to disruptive events and minimize the impact of unexpected incidents on its operations, assets, and stakeholders. This policy applies to all employees, contractors, and stakeholders who have access to or are responsible for critical assets, systems, and business functions.

Roles and Responsibilities

Management

Management provides strategic direction, oversees policy development, approves the final policy, and allocates resources for implementation. They also make critical decisions during emergencies, authorizing the activation of the contingency plan and providing guidance to the response teams.

Information Security

Information Security is essential in contingency planning as it focuses on assessing risks and vulnerabilities related to information assets. Information Security professionals identify potential threats to sensitive data and critical systems and design comprehensive contingency plans to address these risks. They implement security controls to safeguard information assets during incidents and guide incident response efforts to mitigate the impact of security breaches. Additionally, they conduct training

and awareness programs to ensure that employees understand their roles and responsibilities in the contingency plan.

System Administrators

System Administrators focus on the resilience of IT systems in contingency planning. They design system-specific continuity plans, outlining procedures for data backup, recovery, and failover. System Administrators regularly monitor the IT systems for anomalies or incidents and promptly report any issues to the Incident Response Team. They implement backup measures to ensure data integrity and system availability during contingencies. Conducting tests and exercises, they verify the effectiveness of system-specific contingency plans. System Administrators also ensure that the systems are well-maintained and updated to reduce vulnerabilities and support seamless recovery processes.

NIST security controls

CP-1 Policy and Procedures

The City of Milwaukee shall establish and implement comprehensive policy and procedures for configuration management. This policy shall be documented and communicated to relevant personnel or roles within the organization. It will address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements.

CP-2 Contingency Plan

The City of Milwaukee recognizes the significance of contingency planning and is dedicated to its implementation to ensure operational readiness and resilience. The contingency plan shall be integrated with other relevant plans, such as disaster recovery, incident response, and emergency response plans, to create a comprehensive and cohesive approach to managing potential disruptions.

Within the contingency plan, well-defined procedures shall be established to enable the prompt resumption of mission-critical and essential business functions following a disruption or disaster. These procedures shall prioritize functions and outline the necessary steps for recovery.

To support these efforts, a comprehensive assessment shall be conducted to identify critical assets, including information systems, data, infrastructure, and personnel. The contingency plan shall document these assets and outline measures to protect, recover, and restore them in the event of an incident.

CP-3 Contingency Training

The City of Milwaukee shall provide regular training programs to employees involved in contingency planning and response efforts. Training shall cover roles, responsibilities, and procedures outlined in the contingency plan. Additionally, it shall incorporate simulations and exercises to enhance preparedness and improve the organization's ability to effectively respond to disruptions.

CP-4 Contingency Plan Testing

The City of Milwaukee shall coordinate the testing of the contingency plan with related plans to ensure interoperability and effectiveness in various scenarios. Test scenarios should align with identified risks, threats, and vulnerabilities.

CP-6 Alternate Storage Site

The City of Milwaukee shall identify and maintain an alternate storage site that is geographically separated from the primary site. This separation mitigates the impact of site-specific disruptions or disasters. The alternate storage site shall be readily accessible to authorized personnel and equipped with the necessary infrastructure, connectivity, and resources to support recovery and restoration activities.

CP 9 System Backup

The City of Milwaukee shall regularly test the reliability and integrity of system backups to ensure their effectiveness in restoring critical data and applications. Testing should include full and partial data restoration scenarios, and results should be documented for evaluation and improvement.

Cryptographic protection mechanisms shall be implemented to safeguard system backups from unauthorized access, tampering, or data breaches. Encryption algorithms, key management procedures, and access controls should be applied.

CP-10 System Recovery and Reconstitution

The City of Milwaukee shall establish procedures for the recovery of in-progress transactions and the reconciliation of data during system recovery and reconstitution efforts. These procedures should minimize data loss, maintain data consistency, and ensure the integrity of recovered transactions.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

Identification and Authentication Policy

NIST Reference:	Implementation Date :	Revision Number :
IA-Identification and Authentication	June 6, 2019	2.0

Identification and Authentication

Purpose

The Identification and Authorization policy establishes a framework for the identification, authentication, and access control of organizational and non-organizational users to City information systems and resources. The primary objective is to safeguard sensitive data, prevent unauthorized access, and ensure the integrity of user identities within the City's infrastructure.

Scope

This policy is applicable to all employees, contractors, and authorized personnel who access, use, or manage the City's information systems, applications, and data. It covers all information systems owned or operated by the City, whether they are located on-site or accessed remotely. The policy extends to all system components that process, store, or transmit sensitive information on behalf of the City.

Roles and Responsibilities

Management

Management holds the overall responsibility for the effective implementation of this policy. They provide strategic direction, support, and resources necessary for IAM practices within the City of Milwaukee. Management is accountable for risk management, decision-making, and addressing IAM incidents and breaches.

Information Security

The Information Security team configures and manages the logging systems responsible for recording access activities. They diligently monitor access logs, analyze access patterns, and promptly detect any unusual or suspicious activities. In case of security incidents and breaches, the Information Security professionals conduct thorough investigations to identify the root cause and provide actionable recommendations for enhancing access controls and preventing similar incidents in the future.

System Administrators

System administrators are responsible for the day-to-day management of user accounts, authentication mechanisms, and access controls. They enforce password policies, configure multi-factor authentication, and ensure appropriate access rights for users based on their roles and responsibilities.

NIST security controls

IA-1 Policy and Procedures

The City's Policies and Procedures for Identity and Access Management (IAM) shall govern all system operators, managers, and information system providers. These policies and procedures mandate the enforcement of user accountability, implementation of robust user and device identification and authentication measures, and effective management of identifiers and authenticators for users and devices. The objective is to ensure the traceability of system activities to specific users or approved user groups, minimize unauthorized access, and safeguard sensitive data within City information systems.

IA-2 Identification and Authentication (Organizational Users)

Information systems shall be configured to uniquely identify and authenticate all organizational users. Multi-factor authentication (MFA) shall be implemented for both privileged and non-privileged accounts, enhancing access security and minimizing the risk of unauthorized access. Furthermore, access to accounts shall be made replay-resistant to prevent malicious activities.

IA-3 Device Identification and Authentication

Authentication to information systems is defined specific to devices and/or type of devices before connections are established. Dynamic addresses are allocated as defined in the DHCP Scope with a lease duration of 8 days. DHCP audit logging shall be enabled.

IA-4 Identifier Management

ITMD shall ensure that all information systems, to include cloud provided services, do the following:

- Receive authorization from a designated agency representative (e.g., system administrator, technical lead, or system owner) to assign individual, group, role, or device identifiers.
- Select and assign information system identifiers that uniquely identify an individual, group, role, or device. Assignment of individual, group, role, or device identifiers shall ensure that no two users or devices have the same identifier.
- Disable identifiers after 120 days of inactivity, except as specifically exempted by management.
- Delete or archive identifiers that have been disabled more than 365 days.

IA-5 Authenticator Management

The City shall manage information system authenticators by verifying, as part of the initial authenticator distribution;

- The identity of the individual, group, role, or device receiving the authenticator.

- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
- Changing default content of authenticators prior to information system installation.
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.
- Protecting authenticator content from unauthorized disclosure and modification.
- Requiring individuals to take specific security safeguards to protect authenticators.
- Changing authenticators for group/role accounts when membership to those accounts change. Password-based authentication:
- Enforces minimum password complexity of 8 characters, mix of upper-case and lower-case letters, numbers, and symbols.
- Store and transmit only cryptographically protected passwords.
- Prohibit password reuse for 24 generations.
- Allow the use of a temporary password for system logons with an immediate change to a permanent password.
- The City requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.
- Passwords shall not be revealed to anyone, including supervisors, help desk personnel, security administrators, family members or co-workers.

For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

IA-6 Authentication Feedback

To enhance security and prevent unauthorized access or exploitation, feedback provided during the authentication process shall be obscured, ensuring that authentication information remains protected. Specifically, passwords shall be masked upon entry to prevent any accidental or intentional disclosure.

IA-7 Cryptographic Module Authentication

With the knowledge that Cryptographic Module Authentication is a crucial element of information security, guaranteeing the integrity, reliability, and effectiveness of cryptographic modules utilized to safeguard sensitive data and communications, the City shall:

- Utilize cryptographic modules that meet the FIPS 140-2 or higher standard. These modules shall undergo regular security assessments and audits to ensure compliance and effectiveness.
- Employ strong encryption algorithms, such as AES-256 and RSA, to protect sensitive information during storage and transmission. Secure key management practices will also be implemented to safeguard cryptographic keys.

- Require City personnel accessing systems with sensitive data to undergo multi-factor authentication (MFA). This process combines multiple authentication factors, like passwords, smart cards, and biometrics, to enhance security and prevent unauthorized access.
- Restrict access to cryptographic modules, keys, and sensitive data to authorized personnel based on job roles and responsibilities. Regular reviews of access permissions will be conducted to ensure appropriateness and prevent unauthorized access.

IA-8 Identification and Authentication (Non-Organizational Users)

The City of Milwaukee shall identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

- Creating and maintaining access profiles based on user roles, specifying the level of access granted to each user category to ensure that access is limited to the necessary resources for their tasks.
- Establishing a standardized process for onboarding non-organizational users and enrolling them into the appropriate access profiles.
- Implementing a robust authentication process for non-organizational users, utilizing the approved external authenticators for identification.

IA-11 Re-authentication

Re-authentication mechanisms shall be employed to periodically verify the identity of users during extended sessions or sensitive activities.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

Incident Response Policy

NIST Reference:	Implementation Date :	Revision Number :
IR – Incident Response	June 6, 2019	2.0

Incident Response Policy

Purpose

The Incident Response Policy aims to enhance the availability of City resources, rapidly detect incidents, minimize losses due to destruction, mitigate exploited weaknesses, and promptly restore computing services in the event of information security incidents. The policy sets the foundation for a proactive and coordinated incident response approach, ensuring the City can effectively handle and mitigate potential cybersecurity threats.

Scope

This policy applies to all City of Milwaukee personnel involved in identifying, responding to, reporting, assessing, analyzing, and following up on suspected information security incidents concerning information systems and supporting infrastructure. This includes employees, contractors, and other individuals with access to City resources. Additionally, this policy covers all City-owned information systems and any external systems accessed or utilized by City personnel in the course of their duties.

Roles and Responsibilities

Security Team

The Security Team is responsible for overseeing the implementation and compliance of this Incident Response Policy. The Security Team shall ensure that incident response procedures are regularly reviewed, updated, and communicated to relevant personnel. They will also coordinate incident response efforts with appropriate stakeholders and oversee incident response testing exercises.

Incident Response Team

The Incident Response Team (IRT) shall consist of designated personnel from various City departments and agencies. The IRT will be responsible for incident detection, analysis, containment, eradication, and recovery efforts. The team will be led by the CISO or a designated incident response manager. The IRT

members shall undergo incident response training to ensure their readiness and effectiveness in handling incidents.

Department Heads and Managers

Department heads and managers shall ensure that their personnel receive incident response training based on their assigned roles and responsibilities. They shall also enforce the reporting of suspected incidents to the Incident Response Team promptly.

IT Administrators and Technicians

IT administrators and technicians shall play a crucial role in incident monitoring, detection, and containment. They will work closely with the Incident Response Team to provide technical support and facilitate the execution of incident response actions.

Users

All City personnel shall be responsible for promptly reporting any suspected information security incidents to the designated incident response contacts. They shall cooperate with the Incident Response Team during incident investigations and follow established incident handling procedures.

Incident Response Coordinator

The Incident Response Coordinator shall be designated by the CISO or incident response manager and will act as the central point of contact during incident response efforts. The coordinator will ensure effective communication, coordination, and documentation of incident response actions.

NIST security controls

IR-1 Policy and Procedures

The City shall establish comprehensive incident response policies and procedures that outline roles, responsibilities, and guidelines for incident response activities. These policies will provide clear instructions on how to detect, analyze, respond to, and recover from security incidents, ensuring a consistent and coordinated approach.

IR-2 Incident Response Training

City departments shall provide incident response training to personnel based on their assigned roles and responsibilities. Training will cover incident detection, reporting procedures, containment measures, eradication techniques, and recovery strategies. It will ensure that all personnel are well-equipped to handle incidents effectively and minimize their impact on City operations.

IR-3 Incident Response Testing

The City shall conduct regular incident response testing exercises to evaluate the effectiveness of the incident response plan and procedures. These exercises will include simulated incident scenarios and coordination with related plans, such as disaster recovery and business continuity plans, to assess the City's overall preparedness for cybersecurity incidents.

IR-4 Incident Handling

City personnel will follow predefined incident handling procedures to promptly respond to security incidents. Incident handlers will employ containment measures to prevent further damage, identify the root cause of the incident, and implement measures for eradication and recovery. The City will maintain incident response metrics to measure the efficiency and effectiveness of incident handling efforts.

IR-5 Incident Monitoring

The City will implement a robust incident monitoring system to proactively detect and respond to potential cybersecurity incidents. Continuous monitoring of networks and systems will be performed to identify suspicious activities, unauthorized access attempts, and unusual behavior that may indicate a potential security breach.

IR-6 Incident Reporting

City departments and agencies shall establish clear incident reporting procedures to ensure timely and accurate reporting of all suspected information security incidents. Automated reporting mechanisms will be utilized where possible, streamlining the reporting process and facilitating swift incident response actions. The City will maintain records of reported incidents for analysis and improvement purposes.

IR-7 Incident Response Assistance

The City shall establish procedures for providing and receiving incident response assistance to and from relevant entities. This may include collaboration with other government agencies, law enforcement, or private-sector partners. An automated SIEM/SOAR solution will be employed to ensure the availability of information and support during incident response efforts.

IR-8 Incident Response Plan (IRP)

The City shall maintain an up-to-date Incident Response Plan (IRP) that serves as a comprehensive guide for implementing an effective incident response strategy. The IRP will define reportable incidents, establish metrics for measuring risks and priorities, set crisis communication standards, and provide a roadmap for managing and maturing the City's incident response capability. The plan will be reviewed and updated annually to address emerging threats and changes in the City's technology environment.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Maintenance Policy**

NIST Reference:	Implementation Date :	Revision Number :
MA– Maintenance	June 6, 2019	2.0

Maintenance Policy

Purpose

The purpose of this Maintenance Policy is to establish a framework for the systematic and secure maintenance of information systems within the City of Milwaukee. The policy aims to ensure the continuous functionality, integrity, and availability of our information assets.

Scope

This policy applies to all information systems owned or operated by the City of Milwaukee, including hardware, software, networks, and associated equipment. It encompasses all personnel, contractors, and vendors involved in the maintenance, monitoring, and support of these information systems.

Roles and Responsibilities

Management

Management provides strategic direction, oversees policy development, approves the final policy, and allocates resources for implementation.

Information Security

Information Security is entrusted with monitoring and enforcing strict compliance with this Maintenance Policy throughout the organization. They will continuously assess the effectiveness of maintenance procedures and controls by conducting periodic audits. These audits are vital to identifying any potential vulnerabilities or deviations from security standards, allowing for timely corrective measures to be implemented.

System Administrators

System Administrators perform routine maintenance tasks, which include installing updates, patches, and configurations based on the organization's predetermined maintenance schedule. Additionally, the System Administrator document all maintenance activities and maintain a comprehensive maintenance

log. In the event of any maintenance-related incidents or issues, they will promptly report such occurrences as part of the change management process.

NIST security controls

MA-1 Maintenance Policy and Procedures

The City of Milwaukee shall establish and maintain a comprehensive Maintenance Policy and associated procedures that govern all maintenance activities within the organization. This policy will outline the principles, rules, and responsibilities for maintenance personnel and serve as a guiding document for all maintenance-related tasks. The procedures will include detailed steps for planning, approving, and executing maintenance activities, ensuring consistency and adherence to security standards.

MA-2 Controlled Maintenance

To ensure the integrity and security of our information systems, the City shall implement a controlled maintenance process. This process will include detailed procedures for planning, authorizing, and documenting maintenance activities on our systems. All maintenance tasks will be conducted in accordance with approved change management procedures and scheduled maintenance windows to minimize potential disruptions and security risks.

Information necessary for creating effective maintenance records should include:

- The date and time of Maintenance
- Name of individual(s) responsible for the maintenance.
- A description of the maintenance performed. This should include details of system components/equipment removed or replaced including serial or part numbers.

MA-3 Maintenance Tools

To facilitate effective maintenance activities, the City shall employ approved maintenance tools that meet our security requirements and standards. These tools will undergo rigorous evaluation and testing before deployment to ensure they do not introduce vulnerabilities or compromise the security of our systems. Detailed inventories of maintenance tools shall be maintained, and regular inspections will be conducted to verify their integrity and validity.

MA-4 Nonlocal Maintenance

Nonlocal maintenance activities, including remote access to information systems for maintenance purposes, shall be strictly regulated to prevent unauthorized access and potential security breaches. All nonlocal maintenance sessions must be approved and closely monitored by designated personnel. Strong authentication and encryption mechanisms will be employed to secure communication channels during nonlocal maintenance sessions.

MA-5 Maintenance Personnel

Maintenance personnel shall undergo thorough background checks and receive appropriate training on security policies, procedures, and best practices before being granted access to information systems. Access privileges will be based on the principle of least privilege, granting only the necessary permissions required to perform their specific maintenance tasks. Additionally, periodic security

awareness training will be provided to keep maintenance personnel informed about evolving security threats and maintenance-related risks.

MA-6 Timely Maintenance

Maintenance activities will be conducted in a timely manner to ensure the ongoing health and security of our information systems. Scheduled maintenance windows will be established to minimize disruptions to operations, and urgent maintenance tasks will be addressed promptly to mitigate potential risks and vulnerabilities. Delays or deviations from maintenance schedules will be documented and communicated to relevant stakeholders with appropriate justifications and remediation plans.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

Media Protection Policy

NIST Reference:	Implementation Date :	Revision Number :
MP – Media Protection	June 6, 2019	2.0

Media Protection Policy

Purpose

The Audit and Accountability Policy plays a crucial role in upholding the City of Milwaukee's commitment to safeguarding information and critical resources. Its primary objective is to establish a comprehensive plan that effectively addresses incidents and minimizes the impact on City assets. This policy specifically focuses on managing risks associated with insufficient event logging and transaction monitoring.

Scope

The scope of this policy applies to any electronic or physical media containing sensitive City data while being stored, accessed, or physically moved from a secure location. This policy applies to any authorized person who accesses stores, and/or transports electronic or physical media.

Roles and Responsibilities

Management

Management provides strategic direction, support, and resource allocation for effective media protection. They communicate its importance, oversee policy implementation, and reinforce a culture of awareness and compliance.

Information Security

Information Security is responsible for implementing and enforcing media protection measures to safeguard sensitive information stored and transported on various media formats. They play a crucial role in developing and maintaining media protection policies, procedures, and controls to ensure compliance with regulatory requirements and industry best practices. Information Security conducts risk assessments and vulnerability analyses to identify potential threats to media security and devises strategies to mitigate these risks effectively. They also monitor and respond to security incidents related to media, such as unauthorized access or data breaches, and take immediate remediation actions.

System Administrators

System Administrators are responsible for managing the security and access controls of IT systems that utilize media to store and process sensitive information. They work closely with Security to implement media protection policies and ensure the secure handling of media within the IT infrastructure. System Administrators configure and maintain access controls, encryption mechanisms, and logging functionalities to protect media from unauthorized access or tampering. System Administrators also play a key role in media disposal, ensuring that sensitive information is adequately sanitized from media before disposal or reuse.

NIST security controls

MP-1 Policy and Procedures

The City of Milwaukee shall establish a comprehensive Media Protection Policy and associated procedures to govern the handling, storage, transport, and sanitization of all media within the organization. This policy will outline the principles and rules for media protection, addressing the secure use and disposal of media assets. The procedures will provide detailed steps for media management, including access control, marking, storage, transport, sanitization, and authorized use.

MP-2 Media Access

Access to media containing sensitive information shall be strictly controlled. The City shall implement a system of access controls that limit media access to authorized personnel only. Individuals granted access to media shall undergo appropriate security training and be assigned access privileges based on the principle of least privilege. All access activities will be logged and regularly reviewed to monitor for unauthorized access attempts or potential security breaches.

MP-6 Media Sanitization

Media containing sensitive information must undergo secure sanitization before disposal or reassignment to align with compliance requirements. The City of Milwaukee will establish a comprehensive media sanitization process that adheres to industry-recognized standards, ensuring that data remnants cannot be recovered. Sanitization methods will be tailored to the media type and the sensitive information it holds, guaranteeing the preservation of data confidentiality during the disposal or reuse process.

MP-7 Media Use

The use of media for handling sensitive information shall adhere to strict guidelines and authorization controls. The City shall establish policies and procedures to ensure that media use is restricted to approved purposes and authorized personnel only. Any deviations from established media use guidelines must be appropriately documented and approved in advance. Regular monitoring and review of media usage will be conducted to detect and address any potential misuse or security incidents promptly.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

Personnel Security Policy

NIST Reference:	Implementation Date :	Revision Number :
PS: Personnel Security	June 6, 2019	2.0

Personnel Security Policy

Purpose

The purpose of this Personnel Security Policy is to ensure the effective management of personnel-related security measures, aiming to safeguard sensitive information, critical assets, and the overall security resilience of the city.

Scope

This Personnel Security Policy applies to all personnel, including employees, contractors, and third-party individuals, within the City of Milwaukee.

Roles and Responsibilities

Management

Management plays a vital role in endorsing and supporting the implementation of personnel security measures. They provide high-level direction, allocate necessary resources, and demonstrate commitment to maintaining a secure environment. Management ensures that the Personnel Security Policy aligns with the city's overall security strategy and regulatory compliance.

Information Security

The Information Security team is responsible for overseeing the implementation and enforcement of the Personnel Security Policy. They provide expertise on security awareness training and monitor compliance.

System Administrators

System Administrators have a direct role in enforcing access controls and access agreements. They manage access to city systems, databases, and applications, ensuring that only authorized personnel have appropriate access. System Administrators collaborate with Information Security to promptly

revoke access upon personnel termination and manage access adjustments during personnel transfers. They play a critical role in maintaining the integrity of city systems in accordance with security measures.

NIST security controls

PS-1 Personnel Security Policy and Procedures

The city shall create and uphold a personnel security policy and associated procedures that outline roles, responsibilities, and actions pertaining to personnel security management.

PS-4 Personnel Termination

An established procedure shall dictate the prompt revocation of access for personnel upon termination, preventing unauthorized access to city systems and sensitive information.

PS-5 Personnel Transfer

When city personnel are transferred to different roles or departments, their access permissions shall be reviewed and adjusted according to their new responsibilities.

PS-6 Access Agreements

City employees granted access to sensitive information or systems shall sign access agreements, acknowledging their responsibility for safeguarding city assets.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

Physical and Environment Protection Policy

NIST Reference:	Implementation Date :	Revision Number :
PE-Physical and Environmental Protection	June 6, 2019	2.0

Physical and Environmental Protection Policy

Purpose

The Physical and Environmental Protection Policy is integral to the City of Milwaukee's commitment to safeguarding its information systems and critical resources. Its primary objective is to establish a comprehensive plan that ensures a secure and resilient physical environment, protecting against unauthorized access, environmental hazards, and potential incidents.

Scope

This Physical and Environmental Protection Policy applies to all personnel, including employees, contractors, and visitors, who have access to the organization's physical facilities, information systems, and assets. It encompasses all locations where the organization's IT resources and sensitive information are housed, including data centers, server rooms, network closets, and remote offices. The policy extends to cover all aspects of physical access control, environmental controls, fire protection, emergency power, and water damage protection measures. It also includes monitoring and surveillance practices to detect and respond to potential physical security incidents.

Roles and Responsibilities

Management

Management holds ultimate accountability for the implementation, enforcement, and continuous improvement of this Physical and Environmental Protection Policy. They shall provide the necessary resources, support, and commitment to ensure the organization's physical security measures align with business objectives and industry best practices. Management is responsible for appointing key personnel to oversee and execute the policy's requirements.

Information Security

The Information Security team is responsible for developing and enforcing policies, procedures, and guidelines related to physical and environmental protection. They shall collaborate with the Physical Security Manager and Facility Management Team to ensure proper integration of physical and IT security measures. The Information Security team will conduct risk assessments, security audits, and provide recommendations for mitigating physical security risks.

System Administrators

System Administrators are tasked with implementing and managing access control mechanisms for IT resources, ensuring proper configuration of card readers, biometric systems, and encryption protocols for data transmission. They shall promptly revoke access rights for terminated or transferred employees and regularly review access control lists to align with the principle of least privilege.

Facility Management Team

The Facility Management Team is responsible for managing physical access to the organization's facilities. They issue and revoke access credentials based on documented authorizations, maintain access control lists, and oversee visitor access. The team conducts periodic reviews of access privileges and promptly removes access for terminated or transferred personnel.

NIST security controls

PE-1 Policy and Procedures

The City of Milwaukee shall establish and maintain comprehensive policies and procedures for physical and environmental protection. These documents shall define roles, responsibilities, and best practices related to access control, surveillance, emergency response, and protection against physical and environmental hazards. Regular reviews and updates of these policies and procedures shall be conducted to reflect the evolving threat landscape and organizational requirements.

PE-2 Physical Access Authorizations

Access to physical areas and facilities shall be granted based on the principle of least privilege. Authorized individuals shall receive access authorizations tailored to their job responsibilities.

Authorization credentials (e.g., badges, identification cards, and smart cards) shall be issued to everyone accessing a restricted area. The level of access provided to everyone shall not exceed the level of access required to complete the individual’s job responsibilities.

The level of access shall be reviewed and approved before access is granted.

- Keys, badges, access cards, and combinations shall be issued to only those personnel who require access.
- Access rights shall be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides.
- Departments will develop, approve, and maintain a list of individuals with authorized access to the facility or designated area where information systems reside.

- A periodic physical access review is conducted at least annually.

PE-6 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.

PE-8 Visitor Access Records

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

Visitor access records for agency owned computing facilities shall address the following requirements:

- Name and organization of the person visiting.
- Time and date of visit's arrival and departure.
- Name of person visited.
- Signature of the visitor.

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.

PE-9 Power Equipment and Cabling

Power equipment and cabling (power and data) shall be secured and managed to prevent unauthorized access and tampering. Regular inspections shall be conducted to identify and address potential hazards.

PE-10 Emergency Shutoff

The Department of Public Works (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.

PE-11 Emergency Power

Critical information technology systems shall be protected from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems continue to perform during power outages and electrical anomalies (e.g., brownouts and power spikes).

The three primary methods for providing continuous power are as follows:

- Multiple electric feeds to avoid a single point of failure in the power supply.
- Uninterruptible power supply (UPS)
    - Use of a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges. Note: Most UPS batteries do not last for more than four (4) hours without a continuous supply of power.
    - Contingency plans that include procedures to follow if the UPS fails.

    - Periodic inspections of UPS equipment to ensure that the equipment can sustain, for a pre-defined period, the power load of the systems and equipment it supports and is serviced according to the manufacturer's specifications.
- Backup generator(s)
    - Shall be used in combination with a UPS when requirements demand high availability and continuous processing.
    - Contingency plans shall include procedures to follow if the backup generator fails.
    - Tests of the generator shall be done at least quarterly following the manufacturer's specifications. This process is handled and recorded by DPW.

PE-12 Emergency Lighting

Emergency lighting shall be installed in all necessary areas to provide sufficient illumination during power failures or emergencies. DPW Facilities shall ensure the proper functioning and maintenance of emergency lighting systems.

PE-13 Fire Protection

Adequate fire protection measures, including fire extinguishers and sprinkler systems, shall be installed, regularly inspected, and well-maintained.

- Where appropriate, fire-resistant storage for documents and media containing information critical to their business function shall be provided.
- Most file cabinets are not fire, smoke, or water safe and a fire-proof safe may not be water safe and may render any information that is stored in the cabinet or safe unusable; therefore, consideration should be given to storing duplicate copies of information at alternate locations.
- Fire extinguishers must be checked annually, and the inspection date must be documented on the extinguisher.
- All fire protection resources must be tested annually in accordance with local or state fire regulations to ensure they can be successfully activated in the event of a fire.
- Fire detection and suppression devices, supported by independent power sources shall be installed and maintained by DPW.

PE-14 Environmental Controls

Automatic temperature and humidity controls shall be implemented and maintained in data centers and other critical areas to prevent harmful fluctuations. Monitoring systems shall include a notification method for HVAC failures.

PE-15 Water Damage Protection

DPW shall supply master shutoff valves that are accessible, working properly, and known to key personnel to protect the information system from damage resulting from water leakage.

PE-16 Delivery and Removal

Procedures shall be established for the secure delivery and removal of assets and equipment to prevent unauthorized access and loss. DPW shall oversee the delivery and removal process, ensuring proper documentation and accountability.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing physical security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure physical environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Planning Policy**

NIST Reference:	Implementation Date :	Revision Number :
PL – Planning Policy	June 6, 2019	2.0

Planning Policy

Purpose

The Planning Policy was established to effectively manage risks associated with inadequate security by implementing a robust security planning program. This policy, along with related security planning procedures, ensures the adoption of best practices in safeguarding the City of Milwaukee's information systems and supporting infrastructure.

Scope

The scope of this policy applies to all employees, contractors, and third-party users who have access to the City of Milwaukee's information systems and data. This policy applies to all locations where the City's information systems and data are stored, processed, or transmitted**.**

Roles and Responsibilities

Management

Management is responsible for providing the necessary support and resources to implement and maintain effective security planning measures. They shall also foster a culture of security awareness and compliance among all personnel.

Information Security

The security team's role in policy planning involves designing and enforcing robust security measures. They develop policies, conduct risk assessments, oversee implementation, and ensure compliance. The team collaborates with incident response, reviews policies, and continuously improves security measures. Their efforts create a secure environment, safeguard sensitive information, and enhance the organization's resilience against security risks.

System Administrators

System Administrators play a critical role in policy planning by implementing and maintaining security policies within their managed systems. They ensure policy compliance through regular assessments and documentation of system configurations. System Administrators support incident response efforts and provide valuable feedback during policy reviews. Their technical expertise and collaboration with other IT teams contribute to the effective implementation of security measures in alignment with organizational policies.

NIST security controls

PL-1 Policy and Procedures

The Security Planning Policy for the City of Milwaukee aims to establish a robust framework for managing risks related to information system security. This policy ensures the development and maintenance of effective security plans for each information system, aligned with the enterprise architecture. The primary objective is to define the authorization boundary and describe the operational context, missions, and business processes of each system. Additionally, the security categorization of information systems, along with supporting rationale, will be clearly articulated. The policy emphasizes the importance of outlining specific security requirements, identifying relevant overlays, and justifying tailoring decisions for security controls. Through this policy, the City aims to enhance the protection of sensitive information, promote secure practices, and ensure the resilience of its information systems against potential security threats.

PL-2 System Security and Privacy Plans

The City of Milwaukee shall develop a security plan for its information systems consistent with the enterprise architecture. The plan shall explicitly define the system's authorization boundary, describe its operational context, including missions and business processes. It should provide the security categorization of the information system, including supporting rationale, operational environment, and relationships with other information systems. The security plan shall consider privacy implications and include privacy controls. It shall also outline the security requirements for the system, identify any relevant overlays if applicable, describe the security controls in place or planned for meeting those requirements, along with the rationale for tailoring decisions. The plan shall be reviewed and approved by the authorizing official or designated representative prior to implementation. The security plan shall be reviewed annually and updated as needed to address changes to the system/environment or identified issues. The plan shall be protected from unauthorized disclosure and modification.

PL-4 Rules of Behavior

Rules of Behavior concerning information and information systems will be made readily available to all individuals requiring access. Role-based security training will be provided to individuals before granting them access to information system resources. Social media and external site/application usage restrictions will also be clearly defined.

PL-10 Baseline Selection

The City of Milwaukee shall establish a baseline selection process to determine the appropriate set of security controls to be implemented based on risk assessments and specific organizational requirements.

PL-11 Baseline Tailoring

The baseline security controls selected will be tailored to meet the unique needs of the City of Milwaukee. The tailoring decisions will be based on risk assessments and approved by the responsible authorities.

Review and Updates

This policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
July 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Program Management Policy**

NIST Reference:	Implementation Date :	Revision Number :
PM: Program Management	May 2019	2.0

Program Management Policy

Purpose

The City of Milwaukee is committed to implementing an effective and well-structured IT Security Program to safeguard our information assets, maintain the confidentiality, integrity, and availability of data, and ensure compliance with relevant laws, regulations, and industry standards. This policy outlines the principles, roles, responsibilities, and processes that guide the management and continuous improvement of our IT Security Program.

Scope

This policy applies to all employees, contractors, third-party vendors, and systems within our organization that handle sensitive information. It encompasses all aspects of information security, including technology, processes, people, and physical assets.

Roles and Responsibilities

Management

Provide clear support and commitment to the IT Security Program's implementation and maintenance. Allocate necessary resources and promote a culture of security awareness.

Information Security

The Information Security role ensures the protection of the organization's information assets, regulatory compliance, and risk reduction by implementing robust security controls, monitoring for threats, responding to incidents, promoting awareness, and collaborating with stakeholders for a strong and secure IT environment.

IT Managers and System Owners

Collaborate with the Information Security Team to implement and maintain security controls within their respective systems (Configuration Management [CM]).

Employees

Comply with security policies, actively participate in training, and report any security concerns or incidents promptly (Security Training and Awareness [AT]).

NIST security controls

Risk Management

Identify and assess information security risks using a structured and repeatable process (Risk Assessment [RA], Risk Management [RM]). Regularly update risk assessments to reflect changes in the threat landscape, vulnerabilities, and organizational priorities.

Security Controls Implementation

Implement a layered approach to security controls based on industry best practices and standards, such as NIST Special Publication 800-53 Revision 5. Apply technical, administrative, and physical controls appropriate for the organization's risk profile (Access Control [AC], System and Communications Protection [SC], Continuous Monitoring [CM], Configuration Management [CM]).

Incident Response and Recovery

Develop and maintain an incident response plan to ensure a timely and effective response to security incidents (Incident Response [IR]). Regularly test the plan through simulated exercises and refine it based on lessons learned.

Training and Awareness

Conduct regular security awareness training for all employees to ensure they understand their roles in protecting information assets (Security Training and Awareness [AT]). Promote a culture of security-conscious behavior throughout the organization.

Monitoring and Evaluation

Implement continuous monitoring of security controls to detect and respond to security events promptly (Continuous Monitoring [CM]). Conduct periodic security assessments and audits to evaluate the effectiveness of the IT Security Program (Security Assessment and Authorization [CA]).

Compliance and Reporting

Regularly review and update the IT Security Program to ensure alignment with evolving threats and regulations (Security Assessment and Authorization [CA]). Report on the program's status, incidents, and improvements to senior management.

Program Improvement

Regularly review and update the IT Security Program based on lessons learned, industry developments, and changes in the organization's risk profile (Risk Management [RM], Security Assessment and Authorization [CA]).

Review and Updates

This Policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security

needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee **Risk Assessment Policy**

NIST Reference:	Implementation Date :	Revision Number :
RA – Risk Assessment	June 6, 2019	2.0

Risk Assessment Policy

Purpose

The Risk Assessment and Response Policy is vital to the City of Milwaukee's commitment to safeguarding its information systems and critical assets. This policy's primary objective is to establish a comprehensive framework that identifies, evaluates, and responds to potential risks, ensuring the confidentiality, integrity, and availability of sensitive information and resources. The policy encompasses a series of controls aimed at conducting risk assessments, categorizing security, monitoring vulnerabilities, and implementing appropriate risk response measures.

Scope

The Risk Assessment and Response Policy applies to all personnel, including employees, contractors, and third-party vendors, who have access to the City of Milwaukee's information systems, assets, and resources. This policy encompasses all information systems and critical assets owned, operated, or managed by the organization. It includes physical, digital, and cloud-based environments where sensitive information is stored, processed, transmitted, or accessed. The policy extends to cover all aspects of risk management, including security categorization, vulnerability monitoring, risk assessment, and risk response. It governs all departments and business units within the City of Milwaukee, ensuring a standardized and proactive approach to identifying, evaluating, and mitigating potential risks to the confidentiality, integrity, and availability of information and resources.

Roles and Responsibilities

Management

Management holds ultimate accountability for the implementation, enforcement, and continuous improvement of this Risk Assessment and Response Policy. They shall provide the necessary resources, support, and commitment to ensure effective risk management across the organization.

Information Security

The Information Security team is responsible for conducting risk assessments, security categorization, and vulnerability monitoring. They shall collaborate with other stakeholders to develop and implement risk response measures.

System Administrators

System Administrators shall actively participate in vulnerability monitoring and scanning activities, ensuring prompt response to identified vulnerabilities.

NIST security controls

RA-1 Policy and Procedures

The City of Milwaukee shall establish and maintain comprehensive policies and procedures for conducting risk assessments and implementing risk response measures. These documents shall define roles, responsibilities, and best practices related to risk assessment, security categorization, vulnerability monitoring, and risk response. Regular reviews and updates of these policies and procedures shall be conducted to reflect the evolving threat landscape and organizational requirements.

RA-2 Security Categorization

Information systems and assets shall undergo a thorough security categorization process to determine the level of protection required based on potential impact levels. The City of Milwaukee shall classify information systems according to defined security categories, enabling the allocation of appropriate resources for security measures and risk response.

RA-3 Risk Assessment

The City of Milwaukee shall perform comprehensive risk assessments to identify potential threats, vulnerabilities, and impacts on its information systems and assets. Risk assessments shall be conducted regularly to adapt to changing circumstances and emerging threats effectively.

RA-3(1) Risk Assessment | Supply Chain Risk Assessment

As part of risk assessments, the City of Milwaukee shall conduct supply chain risk assessments to identify and mitigate potential risks originating from third-party vendors and suppliers.

RA-5 Vulnerability Monitoring and Scanning

Continuous vulnerability monitoring and scanning shall be implemented to identify and assess potential weaknesses in information systems. Regular scanning shall be conducted to detect and address vulnerabilities promptly.

RA-5(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned

The vulnerability scanning program shall be regularly updated to include the latest known vulnerabilities, ensuring a comprehensive assessment of potential risks to the organization's information systems.

RA-5(11) Vulnerability Monitoring and Scanning | Public Disclosure Program

The City of Milwaukee shall establish a public disclosure program to responsibly communicate discovered vulnerabilities to relevant stakeholders, promoting transparency and proactive risk mitigation.

RA-7 Risk Response

Risk response measures shall be implemented based on the results of risk assessments. The City of Milwaukee shall prioritize risk response actions, including risk acceptance, mitigation, transference, or avoidance.

Review and Updates

This Policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

System and Communication Protection Policy

NIST Reference:	Implementation Date :	Revision Number :
SC-System and Communication Protection Policy	June 6, 2019	2.0

System and Communication Protection Policy

Purpose

The System and Communications Protection Policy is established to ensure that communications and data transfers within the City of Milwaukee's information systems are secure and protected. This policy aims to enforce stringent security controls over data transmissions, maintain the confidentiality of sensitive information, protect against potential communication-based threats, and uphold the integrity and availability of the City's communication resources.

Scope

The System and Communications Protection Policy applies to all individuals, including City employees, contractors, and third-party vendors, who interact with or manage communications within the City of Milwaukee's information systems. This encompasses all communication channels, including but not limited to, hardware, software, networks, and application-based communications, whether developed in-house or externally sourced. The policy spans the complete communication life cycle, from initiation to termination, and emphasizes the security measures required during data transfer or any form of communication within the City's systems.

Roles and Responsibilities

Management

Management oversees the strategic alignment of the SC policy with the organization's overall objectives. They allocate resources necessary for its deployment, support its consistent implementation across all system components, and back regular audits to ensure the policy's resilience against evolving threats.

Information Security

The Information Security Team designs, refines, and enforces the SC policy. Their tasks include defining cryptographic standards, monitoring network traffic for irregularities, leading the response to detected system vulnerabilities or breaches, and spearheading training initiatives to bolster system and communication security awareness.

System Administrators

System Administrators serve as the technical force behind the SC policy's practical application. They configure boundary protections, enforce cryptographic mechanisms, manage secure name/address resolution services, and ensure the protection of data at rest. Maintenance of VPNs, firewalls, and other communication barriers, ensuring they align with the SC policy, is also within their domain.

NIST security controls

SC-1: System and Communications Protection Policy and Procedures

The Chief Information Officer (CIO) or equivalent authority shall establish, maintain, and enforce system and communications protection policies and procedures. These policies shall be reviewed and updated at least annually.

SC-2: Application Partitioning

The IT Department shall ensure applications segregate public-facing components from internal components to prevent potential security threats from compromising internal systems.

SC-3: Security Function Isolation

Security functions shall be implemented in separate and isolated environments to prevent potential tampering or bypassing.

SC-4: Information in Shared Resources

Information systems shall prevent unauthorized and unintended information transfer via shared system resources. This entails:

- Ensuring no residual information from prior users is made available to any current users after resources have been released.
- Preventing unauthorized information transfer when system processing switches between different information classification levels.

SC-5: Denial of Service Protection

The City of Milwaukee implements comprehensive measures to counteract Denial of Service (DoS) attacks on its information systems. Key components of these measures include:

- Traffic Management: By default, all inbound traffic is denied. Exceptions are granted based on a rigorous evaluation of the traffic's legitimacy and necessity. This "deny all, permit by exception" approach ensures that only approved and essential traffic can access the City's systems. For this

control, "inbound traffic" refers to all data packets and requests originating from external sources and directed toward the City's networks and systems.

- Regular scans are conducted to detect potential threats such as bots and Trojan horse programs within the network. The scanning process involves:
    - Utilizing updated threat databases to compare active processes and network traffic.
    - Automated and manual analysis techniques to recognize unusual or unauthorized activities.
    - Immediate alert protocols to notify system administrators of potential threats detected.

SC-6 Resource Availability

The IT Department shall ensure resources are effectively allocated to ensure system performance, preventing potential overloads or service interruptions.

SC-7: Boundary Protection

The City of Milwaukee shall ensure the protection of both external and key internal boundaries of critical information systems. This includes:

- Limiting the number of external network connections.
- Implementing managed interfaces for each external telecommunication service.
- Ensuring confidentiality and integrity of information across interfaces.
- Denying network traffic by default.
- Preventing split tunneling for remote devices.
- Routing internal communications to external networks through authenticated proxy servers.

SC-8: Transmission Confidentiality and Integrity

Transmission processes shall ensure the confidentiality and integrity of data. Cryptographic mechanisms compliant with FIPS 140-2 shall be used to prevent unauthorized disclosure.

SC-9 Transmission Confidentiality

Secure transmission methods, such as SSL/TLS or VPNs, shall be used to maintain the confidentiality of data during transit.

SC-10: Network Disconnect

Sessions inactive for thirty (30) minutes or less shall be terminated. A maximum time-out shall occur after twenty-four (24) hours, necessitating reconnection and re-authentication.

SC-11 Trusted Path

Systems requiring high security shall ensure a trusted path for user communication, preventing potential eavesdropping or data tampering.

SC-12: Cryptographic Key Establishment and Management

The City of Milwaukee ensures the establishment and robust management of cryptographic keys within its information systems. Following NIST standards, this control emphasizes the significance of safeguarding keys throughout their lifecycle.

To enhance the control's adaptability and efficacy against evolving threats:

- Key Lengths: Specific minimum key lengths are set and periodically reviewed based on current security standards and recommendations.
- Acceptable Algorithms: The City adopts only recognized and vetted cryptographic algorithms. The list of acceptable algorithms is periodically updated in alignment with security best practices and emerging standards.

SC-13: Cryptographic Protection

The City of Milwaukee shall deploy FIPS-140-2 compliant cryptographic mechanisms to shield information systems and sensitive data.

SC-14: Public Access Protections

Public-facing systems shall have additional security layers and monitoring to protect against potential threats from public users.

SC-15: Collaborative Computing Devices and Applications

For collaborative computing environments, the IT Department shall ensure only authenticated and authorized users have access, with measures in place to prevent data leaks or unauthorized data modifications.

Review and Updates

This Policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC

City of Milwaukee

System and Information Integrity Policy

NIST Reference:	Implementation Date :	Revision Number :
SI: System and Information Integrity	June 6, 2019	2.0

System and Information Integrity Policy

Purpose

The System and Information Integrity Policy sets the guidelines for managing risks related to system changes. Its goal is to ensure that the City of Milwaukee's information systems are free from exploitable flaws or vulnerabilities, and that data integrity and availability are maintained.

Scope

This policy applies to all City of Milwaukee information systems and data, both digital and physical, and encompasses all personnel, including employees, contractors, and third-party vendors.

Roles and Responsibilities

Management

Management shall oversee and ensure compliance with this policy, provide necessary resources, and set strategic directions for system and information integrity.

Information Security

The Information Security team shall implement and monitor integrity controls, ensuring they are effective.

System Administrators

System Administrators are responsible for regular system updates, patching, and maintenance in alignment with this policy.

Programmers

Programmers shall adhere to secure coding practices, ensuring the software they develop is free from vulnerabilities and potential exploits. They must also validate code changes, cooperate with system monitoring efforts, and participate in regular security training.

NIST security controls

SI-1 System and Information Integrity Policy and Procedures

The City of Milwaukee shall establish, maintain, and implement policies and procedures that guide and enforce measures for system and information integrity. This policy shall be documented and communicated to relevant personnel or roles within the organization. It will address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements.

SI-2 Flaw Remediation

The City shall consistently identify, report, and correct information system flaws. Regular updates and patches shall be applied in a timely manner to ensure system security. Flaw remediation shall be incorporated into the configuration management process.

SI-3: Malicious Code Protection

The City shall deploy mechanisms to detect and prevent the execution of malicious code at multiple information system entry points, such as email attachments, web downloads, and removable media. Malicious code protection will be updated whenever a new release is available.

Malicious code protection mechanisms will be configured to perform periodic scans of information systems and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed.

SI-4 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.

SI-5 Security Alerts and Advisories and Directives

The City shall establish processes to receive, generate, and disseminate security alerts, advisories, and directives. Responses shall be timely, ensuring that all affected systems are updated as necessary.

SI-8 Spam and Spyware Protection

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

Review and Updates

This Policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
May 2019	DOA/ITMD	Draft Created.
June 2019	DOA/ITMD	Final Draft Completed
December 2019	DOA/ITMD	Approval of InfoSec Plan from CIMC
February 2021	DOA/ITMD	Adopted by Common Council
September 2021	DOA/ITMD	Reviewed by Security Analyst
September 2023	DOA/ITMD	Policy Updated to NIST 800-53 Rev5
December 2023	DOA/ITMD	Changes Approved by CIMC