CITY OF DUBLIN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER

ADMINISTRATIVE ORDER 9.1
TO: All City of Dublin Employees
FROM: Megan O'Callaghan, City Manager Megan O'Callaghan
SUBJECT: Information Security
DATE: March 29, 2023
New Administrative Order
PROPONENT: Division of Information Technology

1. PURPOSE

A. The purpose of the Information Security Policy is to provide a framework aligned with the NIST Cybersecurity Framework (CSF) for implementing information security standards and controls used throughout the City of Dublin (City). The goal is to protect our residents and employees, and to ensure the confidentiality, integrity and availability of our critical data, network, and information systems which support key infrastructure and operational activities for the organization.

B. Non-compliance with this policy increases risk to the City.

C. This policy is applicable to all information systems and access controls used within the City except for those where customers or third parties dictate the security requirements.

D. Each version of this policy includes forward looking statements about policy, standards and practices as of the date they are ratified by the City of Dublin Information Security Council (ISC). Unless otherwise specified, City of Dublin organizations and departments will be required to take reasonable steps in a reasonable amount of time and commensurate with risk to implement any new control standards identified in policy revisions agreed by the ISC.

2. OTHER POLICIES, STANDARDS, AND GUIDELINES

A. The creation, maintenance and implementation of technical policies, standards and guidelines regarding computer, network and information security are considered an

ongoing process. As such, special topics and rulings regarding technology and its usage within the organization are noted in an updated policy or division-maintained documentation for the above mentioned. The collected minutes and rulings are to be considered for policy updates and established precedent regarding security controls over technology used within the City.

B. NIST CSF is the program framework selected for the City's Information Security program. This help in establishing the structure for program activities and communications.

C. Security Controls and Risk Assessment will adhere to the Center for Internet Security's CIS18 Controls and CIS-RAM Risk Assessment frameworks. CIS18 controls are closely aligned with the NIST 800-53 control framework and are the foundation for implementing security controls within the City's information technology environments. CIS RAM will provide a consistent means for managing and assessing the implementation of security controls.

D. Please note: PCI-DSS, LEADS/CJIS Policies and/or any other industry specific regulations will supersede any standards, guidelines or controls except where this is more restrictive.

3. SCOPE

This policy encompasses all systems, automated and manual, for which the City has administrative responsibility, including systems managed or hosted by third parties on behalf of the City. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4. INFORMATION STATEMENT

A. Organizational Security

(1) Information security requires both an information risk management function and an information technology security function. It is recommended that these functions be performed by a group that includes both high level executives and subject matter experts from critical functions throughout the City.

(2) The Information Technology (IT) Leadership Team will engage divisions to participate in the Information Security Council (ISC), which will be responsible for the risk management function assuring that:

a. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to

the overall strategic goals and objectives of carrying out its core missions and business functions; and

b. the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

(3) The Division of IT will maintain an individual responsible for technical information security function. For purposes of clarity and readability, this policy will refer to the individual, as the Information Security Administrator. This function will be responsible for evaluating and advising on information security risks.

(4) Information security risk decisions must be made through consultation with both function areas described above.

(5) Although some technical information security function may be outsourced to third parties, the City retains overall responsibility for the security of the information that it owns.

B. Functional Responsibilities

(1) Information Security Council is responsible for:

a. evaluating and accepting risk on behalf of the City;

b. identifying information security responsibilities and goals and integrating them into relevant processes;

c. supporting the consistent implementation of information security policies and standards;

d. supporting security through clear direction and demonstrated commitment of appropriate resources;

e. promoting awareness of information security best practices through the regular dissemination of materials provided by the Information Security Administrator/designated security representative;

f. assisting/advising on any revisions regarding Data Classification outlined in AO 9.4;

g. participating in the response to security incidents as needed;

h. complying with notification requirements in the event of a breach of private information;

i. adhering to specific legal and regulatory requirements related to information security;

j. communicating legal and regulatory requirements to the Information Security Administrator/designated security representative; and

k. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

(2) The Information Security Administrator is responsible for:

a. maintaining familiarity with business functions and requirements;

b. establishing and maintaining enterprise information security policy and standards;

c. assessing compliance with information security policies and legal and regulatory information security requirements;

d. developing the security program and strategy, including measures of effectiveness;

e. advising on security issues related to procurement of products and services;

f. escalating security concerns that are not being adequately addressed;

g. disseminating threat information to appropriate parties;

h. participating in the response to potential security incidents;

i. participating in the development of enterprise policies and standards that considers the City's needs;

j. promoting information security awareness;

k. providing in-house expertise as security consultant as needed;

l. advising on secure system engineering;

m. providing incident response coordination and expertise;

n. monitoring networks for anomalies;

o. monitoring external sources for indications of data breaches, defacements, etc.

p. maintaining ongoing contact with security groups/associations and relevant authorities;

(3) IT leadership team is responsible for:

a. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;

b. providing resources needed to maintain a level of information security control consistent with this policy;

c. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;

d. implementing the proper controls for information owned based on the classification designations;

e. providing training to appropriate technical staff on secure operations;

f. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and

g. implementing business continuity and disaster recovery plans.

(4) The workforce is responsible for:

a. understanding the contents of this policy which is necessary to protect the confidentiality, integrity and availability of information entrusted;

b. protecting information and resources from unauthorized use or disclosure;

c. protecting personal, private, sensitive information from unauthorized use or disclosure;

d. abiding by and agreeing to AO 9.2 Technology Use Policy;

e. reporting suspected information security incidents or weaknesses to the appropriate manager and Information Security Administrator/designated security representative.

C. Separation of Duties

(1) To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.

(2) Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.

(3) The audit and approval of security controls must adhere to the City of Dublin's IT change control process, maintaining separation of the audit and implementation of those controls.

D. Information Risk Management

(1) Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.

(2) Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.

(3) The Information Security Administrator is responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

(4) Risk assessment results, and the decisions made based on these results, must be documented.

E. Information Classification and Handling

Please reference AO 9.4, Data Classification and Protection policy

F. IT Asset Management

(1) All IT hardware and software assets must be assigned to a designated business unit or individual.

(2) IT is required to maintain an inventory of hardware and software assets, including all system components at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

(3) Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

G. Personnel Security

(1) The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific City sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the City.

(2) The City will require its workforce to abide by the Technology Use Policy (AO 9.2), and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

(3) All job positions must be evaluated by the department head to determine whether they require access to sensitive information and/or sensitive information technology assets.

(4) For those job positions requiring access to sensitive information and sensitive information technology assets, department heads will identify and communicate suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the City to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the City.

(5) A process must be established within the City to repeat or review suitability determinations periodically and upon change of job duties or position.

(6) Divisions are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

H. Cyber Incident Management

(1) IT must have an incident response plan, consistent standards, to effectively respond to security incidents.

(2) All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the Information Security Administrator, or, designated security representative as quickly as possible.

(3) The Information Security Administrator must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

I. Physical and Environmental Security

Refer to A.O. 1.14 (or contemporary) for detailed information related to City facilities. This section will specifically address Information Technology or areas where sensitive information is processed.

a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.

c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

d. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

J. Account Management and Access Control

(1) All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and IT.

(2) Except as described in the Account Management/Access Control Standard (N:\Work Units\Information Technology\Standards\Account-Management-Access-Control-Standard.docx), access to systems must be provided by individually assigned unique identifiers, known as user-IDs.

(3) Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.

(4) Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

(5) Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.

(6) Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

(7) Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely, and the method of storing has been approved by the Information Security Administrator/designated security representative.

(8) Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be.

(9) Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with the City's missions and business functions.

(10) Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions.

(11) Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use

consistent with policy, that user activities may be monitored, and the user should have no expectation of privacy.

(12) Advance approval for any remote access connection must be provided by the City and an assessment must be performed to determine the scope and method of access.

(13) All remote connections must be made through managed points of entry. All points of entry will be reviewed by the Information Security Administrator/designated security representative.

K. Systems Security

(1) Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.

a. An individual, or group, must be assigned responsibility for maintenance and administration of any system deployed on behalf of the City. A list of assigned individuals or groups must be centrally maintained by the Information Technology Division.

b. Security must be considered as part of a system's lifecycle.

c. All systems must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).

d. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.

e. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.

f. Environments and test plans must be established to validate the system works as intended prior to deployment in production.

g. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).

h. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

(2) Databases and Software (including in-house or third party developed and commercial off the shelf (COTS)):

a. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:

All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed.

b. Where technically feasible, development software and tools must not be maintained on production systems.

c. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.

(3) Network Systems:

a. Connections between systems must be authorized by the executive management of all relevant entities and protected by the implementation of appropriate controls.

b. All connections and their configurations must be documented and the documentation must be reviewed by the information owner or the Information Security Administrator/designated security representative annually, where appropriate, to ensure the business case for the connection is still valid and the connection is still required; and the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.

c. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between Internet accessible systems and internal systems; systems with high security categorizations (e.g., mission critical, systems containing PII); and user and server segments.

d. Network management must be performed from a secure, dedicated network.

e. Authentication is required for all users connecting to internal systems.

f. Network authentication is required for all devices connecting to internal networks.

g. Only authorized individuals or business units may capture or monitor network traffic.

h. A risk assessment must be performed in consultation with the Information Security Administrator/designated security representative before the initiation of, or significant change to, any network technology or project.

L. Collaborative Computing Devices

(1) Collaborative computing devices (e.g. camera, microphone, etc.) must:

a. prohibit remote activation; and

b. provide users physically present at the devices with an explicit indication of use.

(2) Must provide simple methods to physically disconnect collaborative computing devices.

M. Vulnerability Management

(1) All systems must be assessed for vulnerabilities before being installed in production and periodically scanned thereafter.

(2) All systems are subject to periodic penetration testing.

(3) Penetration tests are required annually for all critical environments/systems.

(4) The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the Information Security Administrator/designated security representative for evaluation of risk.

(5) Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

(6) Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the Information Security Administrator/designated security representative. The Director of IT and/or Information Security Administrator must be notified in advance of any such tests. Any other attempts to perform such

vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

(7) Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and always followed to minimize the possibility of disruption.

N. Operations Security

(1) All systems and physical data processing facilities must have documented management processes, and formal incident management procedures. Clearly define the roles and responsibilities of individuals who operate or use these systems and outline the steps to be taken in the event of an information security incident.

(2) System configurations must follow approved configuration standards.

(3) Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

(4) Where the City provides a server, application or network service to another entity, operational and management responsibilities must be coordinated by all impacted entities.

(5) Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed

(6) Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

(7) Controls must be implemented to disable automatic execution of content from removable media.

(8) Controls must be implemented to limit storage of information to authorized locations.

(9) Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.

(10) All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

(11) All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

(12) Systems which can no longer be supported or patched to current versions must be removed.

(13) Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard (N:\Work Units\Information Technology\Standards\Security-Logging-Standard.docx), and record events to provide evidence and to reconstruct lost or damaged data.

(14) Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.

(15) Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.

(16) Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

(17) Contingency plans (e.g., business continuity plans, disaster recovery plans, and continuity of operations plans) must be established and tested regularly.

a. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

b. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

(18) Backup copies of City information, software, and system images must be taken regularly in accordance with the City's defined requirements.

(19) Backups and restoration must be tested regularly. Separation of duties must be applied to these functions where possible.

(20) Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.