CITY OF DUBLIN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER

ADMINISTRATIVE ORDER 9.1
TO: All City of Dublin Employees
FROM: Megan D. O'Callaghan, City Manager Megan O'Callaghan
SUBJECT: Information Security
DATE: July 1, 2025
Supersedes and replaces Administrative Order 9.1. dated March 29, 2023 regarding the same subject.
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. This document establishes the framework from which other information security policies may be developed to ensure that the City of Dublin can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to City of Dublin by its stakeholders, partners, residents and other third parties.

C. Non-compliance with this policy increases risk to the City of Dublin. Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

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

E. The City of Dublin Information Security Policy describes the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to the City of Dublin, business partners, residents and stakeholders.

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 of Dublin.

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

C. 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 regarding 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 functions may be outsourced to third parties, the City of Dublin retains overall responsibility for the security of the information that it owns.

B. **Functional Responsibilities**

(1) Departmental and Divisional Leadership

a. Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of the City of Dublin.

b. Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.

c. Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.

d. Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Information Security Program.

e. Designate an Information Security Administrator and delegate authority to that individual to ensure compliance with applicable information security requirements.

f. Ensure that the Information Security Administrator, in coordination with the Information Security Council, reports annually to Departmental or Divisional Leadership team on the effectiveness of the City of Dublin's Information Security Program.

(2) Information Security Council is responsible for:

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

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;

f. assist/advise on any revisions regarding Data Classification outlined in AO 9.3;

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

h. compliance 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; 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.

(3) 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 of Dublin'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;

(4) 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.

(5) 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

C. **Policy**

(1) City of Dublin maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:

a. Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical and technical controls.

b. Provide value to the way we conduct business and support institutional objectives.

c. Comply with all regulatory and legal requirements, including:

i. State of Ohio breach notifications laws,

ii. PCI Data Security Standard,

iii. Contractual agreements,

iv. All other applicable federal state laws or regulations.

d. The information security program is revised no less than annually or upon significant changes to the information security environment.