City of Dalton, Georgia
Cybersecurity Policy

A. PURPOSE.

(1) The purpose of the Information Security Policy and Guidelines is to effectively and efficiently manage the risks to City of Dalton Government's information assets from all types of threats, whether internal or external, deliberate, or accidental.

(2) Security is critical to the organization's survival. The goal of utilizing information security as an enabler for proper information sharing and the benefits of a strong program, such as increased ease of administration, reduced complexity of the security architecture, transparency to users, and reduced effort on the part of users, not to mention enhanced security.

B. OBJECTIVES.

(1) City of Dalton Government relies on its information and information systems as a crucial and integral part of providing essential services including meeting its legal and moral responsibility to its constituents for balancing the need for public access to government records while ensuring the integrity of information, the confidentiality of private information, and the availability of their information and information systems.

(2) The ultimate goal of a governmental organization's Information Security Program is to establish enterprise-wide security capabilities that will enable it to safely utilize information technology to provide faster, accurate service and better on-line access to constituents; protect the organization from potential losses and improve the stability of systems; and minimize legal and regulatory liabilities.

C. TRAINING.

(1) Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems.

(2) It is the responsibility of every computer user to know what constitutes acceptable use of City of Dalton Government systems, to know the guidelines, and to conduct their activities accordingly.

(3) All employees and third-party vendors shall receive training and supporting reference materials to allow them to properly protect City of Dalton Government information assets before they are granted access.

(4) Security awareness training shall be provided as needed to ensure they maintain the desired level of proficiency.

D. INFORMATION PROTECTION/COMPLIANCE.

(1) Must be balanced with the need for open government, as established in The Georgia Open Records Act O.C.G.A. §50-18-70 et. seq.).

(2) Provides for public access to government information in all forms (written and electronic).

(3) Provides for exemptions to protect certain private or confidential information.

(4) Requires custodians of electronically stored public documents to provide safeguards against document tampering and unauthorized access to information deemed exempt from public disclosure.

(5) Provides authority for the exemption from public disclosure of those computer applications related to protecting the internal security and integrity of a public agency's data information systems.

(6) Annual reviews of the risks to the City's information and information systems and compliance with this Policy shall be performed by the Information Technology Director and reported to the City Mayor and Council to ensure appropriate visibility exists for the protection being applied to our information and information systems.

E. NON-COMPLIANCE. Non-compliance with this Policy by City of Dalton employees and system users is a serious matter and will be dealt with accordingly on a case-by-case basis. Depending on severity of violations and applicable legal statutes, consequences could result in removal of access rights and special system privileges, removal of system access, or, for City employees, disciplinary action to include potential termination of employment. In severe cases of fraud or breach of privacy laws, legal action may be taken.

F. RESPONSIBILITY. The Dalton City Council bears ultimate authority and responsibility for City of Dalton Government's Information Security. As such, the Council has established this Policy and directs City of Dalton Government personnel to implement the Information Security Policy as follows:

(1) The City Administrator shall approve and enforce all information Security Guidelines that have City-wide scope.

(2) The Information Technology Department Director or designee shall be appointed by the City Administrator as the Information Security Officer (ISO) to provide the direction and technical expertise to ensure that City of Dalton Government's information is properly protected.

(3) All City of Dalton Government Directors, Managers, Program Managers, and Supervisors are directly responsible for implementing the Information Security Policy and Guidelines within their areas of responsibility, and for adherence by their staff.

(4) It is the responsibility of each employee to adhere to the Information Security Policy and Guidelines and to ensure that any vendors or visitors that they sponsor also comply.

(5) The Information Security Officer shall review the program for effectiveness, and will report compliance findings to the Dalton City Council on an annual basis.

G. REMEDIATION. The City of Dalton has acquired Cyber Incident Insurance to mitigate any cost and resources required to resolve breaches of Cyber Security in the City. This along with the framework listed below outlines the response of the Information Technology Department. The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk.

(1) Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

(2) Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

(3) Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

(4) Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

(5) Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.