TOWN OF TABER

Information Security

Procedure No.: CS-IT-10	**Council Resolution No.:** N/A
Department: Information Technology	**Authority:** CAO
Effective Date: September 28, 2020	**Revision Date:** September 25, 2023
Review Date: September 2026	**Repealed Date:**
Supersedes: N/A	
Related Policy No.: CS-IT-10	
Related Policy Name: Information Security	

1.0 PURPOSE

1.1 This procedure is intended to identify clear security requirements and controls for the confidentiality, integrity, and availability of the Town's organizational data, information systems and related assets that store, process, or transmit organizational data.

2.0 OPERATING GUIDELINES

2.1 Access Control:

2.1.1 The Town will limit information system access to authorized users.

2.1.2 The Town will limit information system access to the types of transactions and functions that authorized users are permitted to execute.

2.1.3 The Town will control the flow of nonpublic information (NPI) in accordance with approved authorizations.

2.1.4 A formal user on-boarding and termination process must be developed and initiated to allow assignment of rights.

2.1.5 Duties of individuals will be separated to reduce the risk of malevolent activity without collusion.

2.1.6 The Town will employ a role-based access method.

2.1.7 The principle of least privilege will be employed, including for specific security functions and privileged accounts.

2.1.8 Privileged access rights will be allocated in a highly controlled and restricted process. Their usage will also be controlled.

2.1.9 Upon termination of employment, an employee's or external party's user access rights will be revoked.

2.1.10 Unsuccessful logon attempts will be limited.

2.1.11 Password management systems will be interactive and mandate strong passwords.

2.1.12 Any use of utility programs capable of overriding system and application controls will be highly controlled and restricted, if necessary.

2.1.13 Any access to program source code will be strictly prohibited.

2.1.14 Remote access sessions will be monitored and controlled.

2.1.15 Connections to and use of external information systems will be verified, controlled, and limited.

2.1.16 There will be limited use of organizational portable storage devices on external information systems.

2.1.17 The Town will control information posted or processed on publicly accessible information systems.

2.2 Security Awareness Training:

2.2.1 The Town will ensure that end users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

2.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned Information-security-related duties and responsibilities.

2.2.3 Security awareness training will be provided to ensure all parties can recognize and report potential indicators of insider threat.

2.2.4 Upon completion of security awareness training, all employees will be required to sign a declaration that they have completed training.

2.3 Audit and Accountability:

2.3.1 The Town will create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

2.3.2 The Town will ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

2.3.3 Audit information and audit tools will be protected from unauthorized access, modification, and deletion.

2.3.4 Audit functionality management will be limited to a subset of privileged users.

2.4 System Configuration Management:

2.4.1 Configuration baselines and inventories will be established and maintained of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development lifecycles.

2.4.2 The Town will establish and enforce security configuration settings for information technology products employed in organizational information systems.

2.4.3 The Town will analyze the security impact of changes prior to implementation.

2.4.4 The Town will define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

2.4.5 Emergency changes to an information system must be minimally documented and authorized and performed in a controlled manner.

2.4.6 The principle of least functionality will be employed by configuring the information system to provide only essential capabilities.

2.4.7 Networks will be configured to restrict information flow between information systems or components of information systems through the use of access control lists.

2.4.8 The Town will restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.

2.4.9 The Town will apply deny-by-exception (blacklist) processes to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) processes to allow the execution of authorized software.

2.4.10 User-installed software will be controlled and monitored, and local admin rights will be restricted.

2.5 Identification and Authentication:

2.5.1 The Town will authenticate (or verify) the identities of users, processes, or devices as a prerequisite to allowing access to organizational information systems.

2.5.2 Minimum password complexity and change of characters when new passwords are created is enforced.

2.5.3 The Town will prohibit password reuse for a specified number of generations.

2.5.4 Temporary password use for system logons with an immediate change to a permanent password will be allowed.

2.5.5 The Town will store and transmit only encrypted representations of passwords.

2.6 Incident Response:

2.6.1 An operational incident-handling capability will be developed and implemented for all organizational information systems that house or access the Town controlled information.

2.6.2 Incidents will be tracked, documented, and reported to appropriate officials and/or authorities both internal and external to the Town.

2.6.3 To facilitate incident response operations, responsibility for incident-handling operations will be assigned to an incident response team.

2.6.4 Incident response plan will be reviewed and, where applicable, revised on an annual basis. Review will be based on the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plan will be distributed to key stakeholders.

2.7 System Maintenance:

2.7.1 The Town will perform maintenance on organizational information systems.

2.7.2 The Town will provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

2.7.3 Equipment removed for offsite maintenance will be sanitized of any nonpublic information (NPI).

2.7.4 All media containing diagnostic and test programs will be checked for malicious code before the media are used in the information system.

2.7.5 Only pre-authorized personnel are allowed to perform information system maintenance.

2.7.6 Remote maintenance must be authorized, actively monitored, and audited upon completion.

2.7.7 The Town will supervise the maintenance activities of maintenance personnel without required access authorization.

2.8 Media Protection:

2.8.1 The Town will limit access to NPI on information system media to authorized users.

2.8.2 Information system media containing nonpublic information (NPI) will be sanitized or destroyed before disposal or release for reuse.

2.8.3 Cryptographic mechanisms shall be implemented to protect the confidentiality of nonpublic information (NPI) stored on digital media during transport unless otherwise protected by alternative physical safeguards.

2.8.4 When content from the information system is output to some form of media, that content and media must be handled and stored in a secure manner.

2.8.5 The use of portable storage devices (e.g. Flash Drives, External Hard Drives) will be prohibited when such devices have no identifiable owner.

2.8.6 The Town will protect the confidentiality of backup nonpublic information (NPI) at storage locations.

2.9 Physical Protection:

2.9.1 The Town will protect and monitor the physical facility and support infrastructure for information systems.

2.9.2 The Town will limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. These access points will be monitored.

2.9.3 Protection against natural disasters or other malicious attacks, as well as accidental incidents, will be determined and implemented.

2.9.4 The Town should place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.

2.9.5 Equipment will be handled and protected to ensure risks are reduced, preventing potential environmental threats and hazards.

2.9.6 Equipment will be regularly maintained.

2.9.7 Any removal of assets must be done with prior authorization from the right party.

2.9.8 Any unattended equipment must have applicable protection.

2.10 Risk Assessment:

2.10.1 Security risk assessment criteria should be defined in order to produce consistent assessment results.

2.10.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

2.10.3 Remediate vulnerabilities in accordance with assessments of risk.

2.10.4 The Town will determine what needs to be monitored and measured to demonstrate effectiveness of security and overall risk management processes (e.g. incident reporting, and decrease in overall incidents).

2.11 Security Assessment:

2.11.1 The Town will periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

2.11.2 The Town will develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

2.11.3 Information system security controls will be monitored on an ongoing basis to ensure the continued effectiveness of the controls.

2.12 System and Communications Protection:

2.12.1 The Town should implement limitation and controls of network ports, protocols, and services.

2.12.2 Responsibilities and procedures for the management of networking equipment will be established.

2.12.3 The Town will control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

2.12.4 Unauthorized and unintended information transfer via shared system resources should be prevented.

2.12.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from Internal networks.

2.13 System and Information Integrity:

2.13.1 The Town will identify, report, and correct information and information system flaws in a timely manner.

2.13.2 The Town will provide protection from malicious codes at appropriate locations within organizational information systems.

2.13.3 Information system security alerts and advisories will be monitored, and appropriate actions will be taken in response.

2.13.4 The Town will perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

2.13.5 The Town will monitor the information system, including Inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

CHIEF ADMINISTRATIVE OFFICER

Oct. 5/23

DATE