821. Information Systems Security Policy

The City owns and provides information systems and network facilities to assist employees and other users in conducting City business. The following procedures have been established concerning the City's information systems security policy. For purposes of this policy the term "user" includes all permanent and temporary employees, all contractors, subcontractors, consultants, and vendors who are permitted to use the City's information systems for any reason. The term "information system" includes any software, network, peripheral device, computer, or media used to store, transfer, manipulate, or otherwise use information electronically. This also includes any documents in any form, including electronic or printed, used to prepare, support, manage or use an information system. Violation of the provisions of this policy may result in disciplinary action up to and including termination of an employee and/or other appropriate legal action as concerns both employees and other users.

Authorization

.1 Employees/Users shall be responsible to comply with the provisions of this policy, the Oklahoma Computer Crimes Act (OCCA), and any internal departmental security procedures. The OCCA is provided on the City's Intranet site in the Legal Department's document (DOC) library.

.2 Employees/Users will sign an affidavit acknowledging notification and agreement to follow and comply with the OCCA and this policy. The security affidavit will become a part of the employee's personnel file and provides authorization for the employee/user to utilize specific City information system resources as assigned by the department head or designee. Any non-employee user shall be provided a copy of this policy through a sign-off/receipt process by the hiring manager with a copy retained by the hiring manager.

.3 Unauthorized use of any information system, or access by any unauthorized means or any violation of the OCCA or this policy may result in disciplinary action including termination and/or other appropriate legal action as concerns both employees and other users.

.4 All City employees, contractors, support personnel, volunteers, janitorial staff, and any other persons with unsupervised access to areas containing CJIS equipment or data must have a fingerprint based records check conducted within 30 days of employment, appointment, or assignment. Personnel will also be required to have fingerprints reprinted in accordance with The Oklahoma Law Enforcement Telecommunications System (OLETS)/Criminal Justice Information Service (CJIS) requirements.

Authentication

.5 Authentication is a control established for each information system and consists of: (a) identification of a person requesting use and/or being permitted use of the system, and (b) validation of that person's identity such as a password, magnetic card, biometric device, or by some other means.

.6 Employees/Users shall use the identification and validation assigned to them and not divulge it to others or leave it unprotected. Using or attempting to use any other method of authentication or identification is prohibited.

Remote Computing

.7 Remote access is connecting to a City information system where a portion of the physical path is not under City control, dial-up for example.

.8 Employees/Users using remote access shall comply with all provisions of this policy.

.9 In addition to department head authorization to access the City's Wide Area Network (WAN), separate authorization by the IT Department is required for remote access. Employees/Users requiring such access shall contact the Solution Center (918-~~Help Desk (~~596-7070~~1600~~) to receive such authorization.

.10 Programs which emulate a City-networked PC from a remote location are not allowed.

.11 VPN (Virtual Private Network) access shall be granted to exempt employees and only to a limited number of non-exempt employees who have been granted approval by their Department Head and the Personnel Director or his/her designee. If an employee transfers to another position (either within the same department or in another department), it is the responsibility of the department submitting the original request to terminate the employee's VPN access. A separate request for VPN access in the new position should then be completed.

All employees who access the City network through VPN are responsible for ensuring their personal computers are secure, have appropriate and current virus protection and other necessary security software to minimize risk to the City of Tula network. Employees are required to abide by all security and confidentiality policies and procedures when accessing the City network using VPN.

Protection of Information, Detection and Reporting Violations

.12 The Information Technology Governance~~Security~~ Board (ITGB~~ITSB~~) is responsible for establishing security procedures for information systems.

.13 ITGB~~ITSB~~ will establish methods of prevention and detection of security violations and shall investigate suspected violations.

.14 An employee shall be responsible to promptly notify their supervisor of any suspected violations of this policy. Supervisors shall notify the department head as soon as possible concerning any such alleged violation.

.15 As per state and federal requirements, it is the responsibility of the City of Tulsa Information Security Manager to report suspected computer incidents, and/or breach of personally identifiable information, as quickly as possible. The ultimate goals, regardless of incident, are the protection of assets, containment of damage, and restoration of service.

.16 The reported cyber incident will be coordinated by the Oklahoma Cyber Command with the Oklahoma Office of Homeland Security, Information Analysis/Infrastructure Protection Division (OHS IA/IPD) and the Oklahoma State Bureau of Investigation (OSBI).

.17 In the event of an actual or imminent breach, the City of Tulsa Information Security Manager must complete and submit the "Breach of Personally Identifiable Information (PII) Report" to the District Attorney's Council (DAC) and if applicable an OJP Program Manager no later than 12 hours after an occurrence of an actual breach, or the detection of an imminent breach.