821. Information Systems Security Policy

The City owns and provides information systems and network facilities to assist employees and other authorized users in conducting City business. The following section has been established for the safe and secure use of the City's information systems.

Violation of this policy may result in disciplinary action up to and including termination of an employee, and/or contract termination with any contractors, subcontractors, consultants, or vendors, and/or other appropriate legal action as it concerns both employees and other authorized users.

.1 **Definitions**:

Authorized User
All employees, including interns, temporary, emergency, and special qualification personnel employed or under contract for temporary periods, and any temporary situations or assignments, and all contractors, subcontractors, consultants, and vendors who are permitted to use the City's information systems for any reason.

City Device
Any City-owned computing device such as a desktop or laptop computer, smart phones or tablet.

Information System
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.

Management
The department management staff responsible for the employee and/or authorized user.

Initial Security Awareness Training
Security system training required for users within thirty (30) days of having been granted access to City Information Systems and/or devices which should be made available by the IT Department.

Periodic Security Awareness Refresher Training
Security system training required for users at periodic intervals as determined by the IT Department.

Remedial Security Awareness Training
Security system training required for users after having demonstrated disregard for City Information Systems and/or devices which should be made available by the IT Department. Remedial training addresses learning gaps by reteaching basic skills with a focus on core areas.

Security Awareness
Security awareness is the knowledge and attitude members of an organization possess regarding the protection of its information systems assets and resources whether physical or virtual, (online, email, software, internet, etc.) Security

awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches.

.2 Authorization

.21 Employees/Authorized Users are required to comply with the provisions of this policy, the Oklahoma Computer Crimes Act (OCCA), (21 O.S. § 1951 et. seq. as in effect at any given time), any City of Tulsa Information Technology Department published policies, and any internal departmental security procedures. The OCCA and Information Technology Department published policies are provided on the City's Intranet site in the Information Technology/IT Policies & Procedures document (DOC) library.

.22 Employees/Authorized Users will sign an affidavit acknowledging notification and agreement to follow and comply with the provisions of the OCCA and this policy prior to receiving access.

For employee authorized users, the security affidavit will remain on file in the IT department and provide authorization for them to utilize specific City information system resources as assigned by the department head or designee.

All authorized users should be provided a copy of this policy through a sign-off/receipt process administered by the IT Department.

.23 Anyone with unsupervised access to areas containing CJIS equipment or data, whether an authorized user or not, must have a fingerprint-based records check conducted within 30 days of employment, appointment, or assignment. Employees will also be required to have fingerprints reprinted in accordance with The Oklahoma Law Enforcement Telecommunications System (OLETS)/Criminal Justice Information Service (CJIS) requirements.

.3 Authentication

.31 Authentication is a control established for each information system and consists of: (a) username (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 trusted means.

.32 Employees/Authorized Users shall use the username (identification) and validation (password) 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, and for employees is a violation of policy which could lead to disciplinary action up to and including termination.

.4 Remote Computing

.41 Remote Computing is the ability of users to use a computer or other electronic device to connect through the internet to a City information system either through the use of a Virtual Private Network (VPN) or other secure connection method.

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

.43 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/Authorized Users requiring such access shall contact the Solution Center (918-596-7070) to receive such authorization.

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

.45 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.

.451 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.

.452 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.

.5 Protection of Information, Detection and Reporting Violations

.51 The Information Technology Governance Board (ITGB) is responsible for establishing security procedures for information systems.

.52 ITGB will establish methods of prevention and detection of security violations and shall investigate suspected violations.

.53 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.

.54 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.

.55 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).

.56 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.

.6 Security Awareness Training

.61 Due to current threats in the internet sphere, Information Technology Security awareness, precautions, and comprehensive training are all essential and are a responsibility of all parties including the employee/authorized user, management, and the IT Department. Each time a user accesses the network and/or uses a City device, there should be a focus on security and precaution which cannot be compromised.

Failure to follow the directives outlined below may lead to disciplinary action up to an including termination of employment and/or user access.

.62 IT Department Responsibilities

System Access

.621 The IT Department (IT) will be responsible for regular system updates to ensure security measures are in place at all times.

.622 IT may restrict access to sites it deems unsecure, unstable, and/or threatening.

Training

.623 IT will make available initial, periodic refresher, and remedial security training as needed to enable authorized users to understand and practice security awareness.

.624 In order to secure the network, IT may periodically test users for the effectiveness of Security Awareness Training. If an authorized user is determined to act contrary to best practices outlined in Security Awareness training and/or policy, IT will categorize the user as needing remedial training. The user will then have thirty (30) days to complete remedial security training.

.625 Anyone who demonstrate a disregard for security awareness as defined above and/or during training must successfully complete Security Awareness refresher training within the timeframe specified in this policy section.

.626 In its discretion, in order to ensure security and mitigate risk, IT may restrict and/or suspend access to information systems and/or deny the creation or assignment of additional access to an authorized user if the user fails to successfully complete Security Awareness training as assigned, whether initial, periodic refresher, or remedial.

.63 User Responsibilities

.631 All users will be required to complete initial Security Awareness training within 30 days of being granted access to City information systems.

.632 Failure to meet the requirements of Security Awareness training as outlined in policy may result in disciplinary action up to and including termination and/or suspension of the employee's or authorized user's access.

.64 Management Responsibilities

.641 The employee's/authorized user's department is responsible for ensuring all users comply with Security Awareness Training. IT will notify management of any outstanding training needs of its employees.

.642 Failure to meet the requirements of the Security Awareness training as outlined in this policy may result in disciplinary action up to and including termination and/or the IT department placing the user into an unauthorized status, disabling system access as applicable, and/or restricting use of City devices.