D. INFORMATION SECURITY POLICY

PURPOSE

All members of the City organization share some level of responsibility for protecting information resources against system unavailability, service interruptions, identity theft and fraud. In practice, this translates to proper use of passwords, safeguarding City IT equipment, etc. More specifically, the City's Innovation & Technology and Police Departments are jointly responsible day-to-day for the physical protection of the City's information technology systems and electronic data. The purpose of this policy is to identify the authorities and protocol for gathering, keeping and reporting on City data.

POLICY

A position of trust has been conferred upon every authorized person who comes in contact with any data and information to keep it secure and private. All City employees, contractors, vendors and contingent workers are obligated to recognize and adhere to these responsibilities while on or off the job.

Users must acknowledge that it is their responsibility for understanding the confidentiality of the datasets they are working with and that they are responsible for maintaining the level of access when copying data on our network, and especially when uploading data to cloud solutions (Such as ArcGIS Online).

- It is the policy of the City to ensure the ongoing critical City operations by establishing and maintaining proper security of its Information Technology Systems and the data contained therein against system unavailability, service interruptions, identity theft and fraud, criminal or unauthorized attack or disclosure.

- All City information systems must be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within.

- All staff consent to not remove or cause to be removed copies of any official record or report from any file from the office where it is kept except in the performance of his/her duties.

- All staff consent not to use any system, application or cloud based product (such as Amazon S3, Dropbox, Google Docs/Drive/Hangouts, Microsoft Messenger/Windows Azure, Mozy, Rackspace, etc.) for communication, data sharing, processing or storage without explicit approval from the Division of Innovation and Technology (DoIT) or their designate.

- Report any security incidents, potential security risks or vulnerabilities to the Division of Innovation and Technology.

- Acknowledge that information stored on or passed through City computer communications hardware is not considered private. Users of this equipment must not have expectations of privacy of any data or information, including electronic mail and voice mail. All information on and transmitted to or from any computer system or network may be intercepted, recorded, read, copied, and disclosed by, and to authorized personnel, for official purposes, including criminal investigations. Access or use of any computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.

PROCEDURE

General

- All employees must lock their computers [Control-Alt-Delete] when the workstation is left unattended.
- All employees must adhere to the City's password policies and procedures (2.6.2 Password Policy).
- All servers, desktops and laptops connected to the City's network, including those using remote network access, must participate in the Citywide managed antivirus software.
- In order to protect against malicious code, users should be cautious opening any files attached to electronic mail from unknown or un-trusted sources. The legitimacy of any suspect messages should be verified by contacting the sender through an alternate channel such as a direct conversation or a phone call.
- DoIT reserves the right to immediately disconnect any device or agency from the City's network which it deems out of compliance with this policy.

Financial Security Standards (PCI Compliance)

All staff with responsibilities for managing credit card transactions and those employees who are entrusted with processing, transmitting or handling cardholder information in a physical or electronic format must participate in the PCI DSS Program.

All computers and electronic devices involved in processing payment card data are governed by PCI DSS. By adhering to these standards the City's liability is limited and the processing of credit cards may continue.

Data Breach Responsibilities

Any actual or suspected breach in any type of media (e.g., electronic, paper, verbal, microfiche, etc.) must be reported immediately to the Help Desk at helpdesk@cityofredlands.org.

Lost or stolen computers, laptops, tablets, smartphones or other electronic storage media must be reported immediately to helpdesk@cityofredlands.org or techlog@redlandspolice.org.

INNOVATION AND TECHNOLOGY 2.1.4

Data Management Standards

1. When a department requires access to former employee user data:

    - Employee user data is defined as a copy of any files and file folders saved to their desktop and/or personal file drive. Data stored on the shared file drives on the City's network is not applicable since it is already accessible. Email accounts are not explicitly included in this definition. Email is stored automatically for every account for a period of 2 years.
    - The department that is requesting access to a former City employee's files must have authorization from a position at least one level higher than the separated employee.
    - Requests must be sent in writing (email) to Helpdesk@cityofredlands.org and should specify the electronic files requested as specifically as possible.
    - The Department of Innovation and Technology will retain former employee data for a period of 3 years. After that point, the corresponding department will have the opportunity to take possession of the data or to agree that it may be disposed of.
    - Requests will be addressed within 2 business days.
2. When a Notice of Mandatory Preservation of All Documents, Records, E-Mail, And Electronic Data is received:
    - The City Attorney's Office will generate a Communication Memo
    - That memorandum will notice the appropriate departments, specify that data to be preserved and direct the IT department to suspend any normal administrative actions that would result in the accidental deletion of such data.
    - The appropriate departments will receive an email with "Electronic Data Preservation Instructions" that will specify exactly how they are to preserve that data from their computers.
    - Such memorandums will be addressed immediately.
3. In an effort to safeguard the City's network and data:
    - The Department of Innovation and Technology have elected to utilize a website content filter and monitoring software.
    - This software runs in the background on each City computer connected to the City's network.
    - Its sole purpose to prevent malicious attacks on the City's network and to prevent wastes of network bandwidth that has the potential to impede or crash the City's connectivity to its network.

All forms for this policy can be found here: J:\DoIT Forms