



INFORMATION TECHNOLOGY

POLICY & PROCEDURES

TITLE: PROTECTING CONFIDENTIAL INFORMATION

DATE INITIATED: April 17, 2007

DATE APPROVED: July 27, 2007

DATE REVISED: December 1, 2009

TO BE REVIEWED: Annually

RESPONSIBLE PERSON: Deputy Director

SCOPE: Pertains to confidential information under the control of IT Department

POLICY All confidential City information and data must remain confidential and protected from access from within IT and outside of IT. Additional responsibility occurs for legally protected data, such as HIPAA data, employees' identity information, Red Flag data, and Public Safety secured systems and data. In all cases, the responsibility for protecting confidential information rests with those who have access to and/or handle the information and data systems. This includes persons who routinely and appropriately access it during the course of business; those who by the nature and scope of their jobs have access to it; and to everyone who by physical proximity to employees with high security clearance have the ability to see confidential information.

City of Tucson Administrative Directive 1.08-3 establishes a direct responsibility for controlling data access and data integrity within the City. The IT Department has dual primary roles over information, as follows:

- (1) To maintain a highly secure citywide environment that is secured against to external unauthorized access.
- (2) To develop data security standards appropriate to the information within the IT department.

Specific data access requirements are also established by the State, as specified in Arizona Revised Statutes 41-1750 and 41-1756 (which relate to the security of Public Safety data), and 13-2316 (which deals with the definition and criminal penalties for unauthorized computer access). Requirements from other state and federal Public Safety agencies will also be addressed.

Employees who fail to comply with this policy may be subject to discipline as specified in AD 1.08.3 and ARS 13-2136.

DEFINITIONS

ACJIS means the Arizona Criminal Justice Information System rules which pertain to the protection of Public Safety related data.

Background Check means the use of a police background examination to approve people for access to secured systems and data.

Data Vault means an encrypted file system which acts just like another disk drive so that an employee can write to and read from it. However, the particular data in that vault is not available to anyone who does not have the access codes, passwords, or encryption keys.

HIPAA is an acronym for Health Insurance Portability and Accounting Act. This legislation was enacted by Congress in 1996, and its primary intent is to protect a patient's privacy. Any data relating to an individual's health is considered PHI, protected health information, under this act and should be secured and protected.

LASO means the Local Area Security Officer who makes sure that information security practices comply with Arizona Department of Public Safety rules.

Network Scans refers to the use of automated tools to periodically probe and test the security of servers, switches, and data for known security flaws.

Network Security means the ability to use firewalls and other tools to restrict access to both the overall City network, as well as secured sections within that network.

Password Management means the use of a software tool which securely stores all system passwords, enforces password complexity, mandates password changes, and tests all system regularly for security. The program is administered by a security administrator who has Public Safety background clearance.

PHI is protected health information.

Red Flag Rule means an FTC (Federal Trade Commission) program which mandates identity data protection for entities which grant credit or accept payments.

Secure means protected from access within IT (other than necessary access by a limited development or support team), as well as protected from access outside the IT department or the City.

Breach of unsecured PHI occurs where there is an unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of that information, except where the unauthorized person to who the information was disclosed would not reasonably have been able to retain such information. A breach does not include an unintentional disclosure or use by an employee or individual acting under the authority of the covered entity or business associate if the disclosure was made in good faith.

Unsecured PHI Under HITECH 2009 is protected health information not secured through use of a technology or methodology identified by the Department of Health and Human Services.

PROCEDURE

Gaining required individual security clearances

1. All IT employees who work with information systems and/or have access to such systems are required to take security training. This will vary according to the specific job responsibilities of individual positions.
2. All employees are required to take the Public Safety information security class and the HIPAA online training class. Refresher classes must be taken for these items on a periodic basis. These classes cover each individual's responsibility for preventing unauthorized data access.

3. Employees who are required to access Public Safety systems or functions within the Public Safety secured network must pass a thorough police background check, which includes personal history, credit report, and being fingerprinted.
4. Employees with job responsibilities that require routine access to confidential police data must pass a full police background exam, which includes a drug test and a lie detector test.

Most of the data in the IT Department belongs not to IT, but to other City departments who have entrusted this information to IT's care, management, and protection. The responsibility is the same whether the data (1) is in major applications or databases hosted on our servers; (2) is in development environments residing on any hardware (server, desktop, or laptop); , or (3) is either printed out or stored electronically.

Information or data designated as confidential shall not be placed on a shared common drive or on a PC's "C" drive, which have minimal security. This prohibition also applies to a laptop or to any other computer which is accessible outside the City's firewall (including home PCs). Instead, such data is required to be stored in a data vault or data crypt. The data vault acts just like another disk drive so that an employee can write and read from it. However, the particular data in that vault is not available to anyone who does not have the access codes or keys. To request a data vault and receive training in how to use it, contact the IT Help Desk.

Employees should also be aware that hard copies or printouts are subject to the same tight security. Such hard copies, when not in use, should always be under lock and key. Systems administrators, through their management of the server operating systems, can also gain access to confidential information. Access to such data is never a part of individual job duties and should not occur unless specifically directed by an IT Administrator as an exception to normal processes.

PRACTICES

IT has specific practices and programs in place to protect data and access to it. These include:

1. All administrative passwords to City systems must be centrally stored in the IT Department's password manager program. Unless a system has a valid password system stored in the Password Manager, the system will be removed from the network as a security threat.
2. Protecting against external intrusions, penetrations, viruses, malware, and active security attacks are granted the highest level of priority for all City IT resources.
3. People will be denied access to secured systems or data for which they have not received clearance. The only exceptions will be for a person accompanied by an individual with the appropriate security clearance level. A list of staff with security clearance will be maintained in the IT Director's office.
4. IT will conduct regular penetration and security status testing and will cooperate with third parties who need to review such testing or perform their own. Copies of findings and corresponding corrective actions will be retained for not less than one year.
5. IT will never use copies of secured data in doing system testing or system development where the environment is less secure than the production system environment.
6. All PCs used by IT staff will use password protected screen savers, with a maximum wait time of five minutes.

7. All PCs and servers will use City standard anti-virus and malware protection. All PCs and servers will apply standard security patches as approved by the IT security team. Exceptions must be approved by the Director's office.
8. Secured data will never be accessible to or delivered to a vendor until a specific Data Confidentiality Agreement with that vendor has been signed.
9. Any time confidential data needs to be accessed, transported, or stored on a device that is outside the City's firewall, it must be encrypted.
10. Access from outside the secured network firewall to confidential data within the firewall must be made via the City's approved encrypted VPN account.
11. Computers, that will routinely have access to Public Safety secured data, will either be used in locations where the screen cannot be seen readily from outside the workstation or will use approved privacy screen guards.
12. Confidential data and systems will retain secured log file records of all access attempts, whether or not an attempt was successful.
13. Access to servers, switches, and firewalls relating to Public Safety data will be physically restricted to personnel who have the appropriate security clearance. This may occur via either electronic keycard access or physically secured areas with limited key distribution. Persons without Public Safety clearance may enter only when escorted by a person with security clearance.
14. Exceptions to security controls as stated above require director authorization. Such exceptions, if granted, will be for a limited duration and require re-authorization for any extension or renewal.
15. All changes to systems and data access will go through a Change Control process that includes representatives with obligations for the security and integrity of confidential data.
16. IT will periodically (but not less than twice a year) randomly audit staff compliance with security practices and programs
17. Backups of confidential information will be made in encrypted format.
18. The IT department will assign the role of security officer to a member of the staff who has passed the Public Safety background checks. This person may or may not be the same as the Public Safety LASO.
19. The City's Internet connection will support a 128-bit SSL connection.
20. Lifecycle replacements and new acquisitions will be made to comply with current security considerations.
21. The City will maintain software licensing records for all software installed on secured systems.
22. All employees are required to immediately notify their supervisor of a data breach. Supervisors will notify the respective department management. If the data breach involves unsecured PHI, the Tucson Fire Department will notify patients of the breach in accordance with the HITECH Act of 2009. IT will provide all the necessary information that must be disseminated in the required notification.
23. IT will maintain a data breach log for unsecured PHI. IT will work with the Tucson Fire Department in filing any data breaches with the Department of Health and Human Services in accordance with the HITECH Act of 2009.
24. The City will develop and maintain a disaster recovery plan that encompasses and prioritizes the protection and restoration of Public Safety systems and data.