Information Technology Services Department

Security Best Practices and Protecting Sensitive Data Guidelines for new and existing personnel

---

To safeguard your information, your identity and the City of Albuquerque networked systems, it is critical that each of you follow these basic guidelines.

1. Do not copy or download sensitive data (e.g., social security numbers, credit card numbers, health records, and other information protected by law) from the City's networked resources your PC, Web server, PDA, Laptop, or any other portable device.

2. Do not store sensitive information at home. This especially includes system backup tapes.

3. Avoid sending un-encrypted sensitive data via email. Email messages can be intercepted by third parties or mistakenly sent to the wrong address.

4. Protect printed sensitive data. Do no print sensitive data to a public accessible printer. Store sensitive data in a locked desk or cabinet

5. Don't leave unattended sensitive data on the copier, fax or printer. Shred sensitive data that needs to be disposed.

6. Secure your workstation (or logoff your sessions) when you leave your workstation. Don't leave a logged on workstation unattended.

7. Avoid Peer-to-Peer file sharing software. The following software and their clones are prohibited from use: Bittorrent, Audio Galaxy, Kazaa, IMesh, Morpheus, Gnutella, Bearshare, Limewire, Napster, Winmix, Edonky2000, Direct Connect, etc. **(See IT Standard, Peer to Peer internet based applications Prohibited Titles Standards)**

8. Do not download programs, applets and images from unreliable and unknown sources; you might also be downloading Trojans with it.

9. Make sure you sanitize any computer containing sensitive data prior to disposal or transfer of ownership. **(See December 2012 Cyber Security newsletter)**

10. Use antivirus software and update it frequently to keep destructive programs off of your computer.

11. Make sure that you regularly backup any critical data or e-mail that you do not want to lose.

12. Do not open file attachments from an unsolicited email until you confirm the source by contacting the sender. You must have updated antivirus software running all the time.
13. Use a hard-to-guess password that contains a mix of numbers and letters (use mixed case) and change it frequently. **(See IT Password Standard)**

14. Never share passwords with anyone. Use different passwords for different internet sites as you visit them. Make it harder for someone to guess your password by not sticking to a common password or a pattern.

15. Wireless technology has inherent security weaknesses. Therefore, it is highly discouraged to transmit sensitive or critical data over wireless connections. The City has created a secure wireless network for staff. While in City buildings, this secure network should be utilized for any wireless technologies.

16. The city has a secure VPN solution for remote access. Any connection outside of the City infrastructure to obtain access to City networked resources will be provided via VPN.

17. Keep your applications and Operating system up to date on patches. Use the most up to date version of your Web browser, email software and other programs. Update your operating system regularly.