NNEDV

Computers and Networks

How the Technology Works

The term "computer" typically refers to the tower or laptop that holds the processor, hard drive, power, etc. A server is also a computer, often with more memory and more hard drive space. Files are stored on the computer's hard drive, which is a small box about the size of a deck of cards.

Computers can be connected to each other via wired or wireless networks. A network is a group of computers connected either physically by Ethernet cables (and routers, switches, and hubs) or wirelessly via radio signals. Computers are networked in order to access the Internet over a shared connection or to gain access to a shared central server that stores shared files and can allow access to shared calendars and shared printers.

How Are Grantees (Agencies and Partnerships) Using It?

OVW grantees are using computers extensively since computers are the building block of many other technologies grantees use. Computers allow us to log onto the internet to connect to resources, download court forms, use GPS to track offenders, and create and access databases and spreadsheets to keep information organized. Many cell phones are now more like handheld computers, allowing users to check their address book, email, instant message, search the web, and more.

Benefits and Risks

- Computers drastically reduce the amount of physical storage space required at an agency to store documents and records. About 250,000 pages of text (or 500 floppy disks) fit on one CD-ROM (700MB). Computers are now routinely sold with hard drives of 100 GB to 700GB (100,000MB – 700,000MB), so the storage capabilities are endless.
- Computers allow for the creation of court databases, offender management systems, protection order registries, or other databases that allow agencies and organizations to effectively carry out their tasks and responsibilities more efficiently.
- Computer hard drives have the potential to become defective and stop working. If this occurs, all the data stored on that hard drive can be lost instantly. If that hard drive is from an agency's network or server, which holds all the shared files, thousands of files and historical data can also be lost. It is good practice for agencies to have policies in place that promote the practice of doing regular backups to store data to ensure that valuable information is not lost forever.
- Wireless networks are inherently less secure than wired networks because it is easier to intercept information transmitted through the air than information transmitted via a phone line or Internet cable. Encryption is just one of several ways that wireless computer networks can be made more secure; however, even a secured wireless network is not appropriate for highly sensitive information (e.g. personally identifiable victim information).

Things To Consider

Computer Technical Support: While some the technology terms in this short document may seem complex to the average user, this document and the terms used in it may provide assistance to your agency's technology support person. Consider having a conversation about the issues outlined in this document with your technology support staff.

Essentials: Has the agency budgeted for antivirus software and annual renewal of virus definitions? Is the intended use of the computer allowable under OVW grant programs? When purchasing computers, an agency should carefully assess their current and future needs to ensure that the purchased equipment is and will be adequate for the duration of the grant or project. Typically, a computer with a mid-sized hard drive, processor speed, and memory is appropriate. Typically a grantee will not need the most expensive computer but may not want to purchase the cheapest. The agency may also want to consider purchasing an extended warranty.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012

NNEDV

Computers and Networks

Training: The most common challenge of computer software upgrades is user training. Funds should be budgeted for user training on new operating systems (such as MS Windows or Mac OS X) and software programs (such as MS Excel or Adobe Pro). In the past, upgrades were often minor but recent upgrades have produced vast differences in versions.

Disposal: If the agency is purchasing new computers to replace outdated ones, it is important that they do not donate old computers before removing the hard drive. Since no "windows washer" program can fully clean hard drives, most agencies will find it quicker and easier to simply physically remove the hard drive and allow the new owners to replace them. If the agency wants to donate the old computers with the hard drive intact, it is crucial that hard drives are scrubbed by a low-level reformat that meets the U.S. National Institute of Standards and Technology (NIST) standards for data sanitation, which includes magnetically wiping the drive. *(Note: If you inform your tech support person that you need your hard drive reformatted or magnetically wiped to "NIST standard," they should know what this means and be able to effectively clean your hard drive—or you can remove the drive and keep it secured in your office.)*

Cost: Has the agency priced multiple options? Has the agency included the costs of technical support to setup and network the new computers? Has the agency budgeted for maintenance, upkeep, and regular replacement and technology upgrades?

Security: How many different computer networks are or will be housed on site, and what physical and technological security measures will be implemented to protect the computers and networks? Computer monitors in public areas should be arranged to prevent others from accidentally or intentionally viewing confidential victim/client information on computer screens. Password-protected screen savers can be used as an added layer of security when users leave their desks.

Authorized Access & Usernames: Every user should have a separate and unique user name and password. Policies and procedures should be in writing as to how these accounts are established and what technical support resources are available if users forget or lose their passwords. Specifically, how will grantees ensure that users do not sign on using a coworker's account and password if they forget their own passwords? How will the agency know if unauthorized user access occurs? Will the agency keep audit trails?

Backups: How will data be backed up? How often? If electronic backups are stored off site, they should be protected and purged in the same manner and within the same time limits as information stored onsite. Backups of any sensitive and confidential information should be secured, locked, and protected to comply with laws and ensure victim confidentiality.

Security in Co-Located Sites: When law enforcement, attorneys, and advocates share a location, client databases are not allowed to be linked and must function autonomously from each other.

In co-located agencies, it is important to make a distinction between ownership of the equipment and ownership of the data stored on the equipment. This ownership policy should be noted in writing and signed by the appropriate parties. For example, if Agency A has provided a computer for Agency B to use, a written contract should designate that Agency A retains ownership of the hardware (minus the hard drive) and Agency B owns all data and has ownership of the hard drive.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012