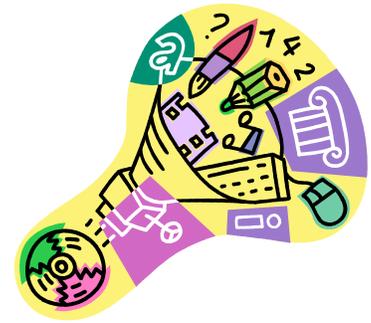


# Information Management

Information management is a set of processes and related technology solutions that enable organizations to understand, organize, and manage all types of data. (e.g., general files, databases, and e-mail. [Adapted from BCS, Business IT Interface]



## Background Check



District employees currently must undergo background investigations and credit checks for use of federal computers. These requirements are based on a federal government-wide directive. All government partners, contractors, and others who have access to government computers must comply. With increasing cyber-crime, this type of extra precaution is necessary for security reasons and applies universally to anyone accessing a federal computer, including district managers. A credit check is a basic security requirement of the federal government and many private businesses. USDA is only interested in the identity portion of the report and not the credit information. In Colorado, NRCS is covering the payment for conducting the background check requirement. USDA can only accept the US Office of Personnel Management (OPM) as the valid source for background investigations.

## Cyber Security

What is cyber security?

In today's technology driven world, we rely on computers and the internet for many aspects of our daily lives, both personal and work-related: — communication (e-mail, cell phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), financial transactions (on-line banking, credit cards), medical records and the list goes on and on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system? Cyber security involves protecting both personal and work-related information stored and accessed by computers and other communication methods.

Here are the TOP 10 simple, easy, and basic things that everyone can and should do to protect their computer systems and data from harm by various cyber attacks and other types of security incidents that can cause damage, consume computer resources, or expose confidential information.

1. Use and regularly update firewalls, anti-virus, and anti-spyware programs. There are many types of Internet security and safety issues that you should defend against. One of the most effective ways of defending your computer is to use a firewall and up-to-date anti-virus and anti-spyware products.
2. Properly set up and patch operating systems, browsers, and other software programs. Whenever security updates or service packs become available for your operating system or programs, it is very important to promptly download them and patch your operating systems and programs. These patches are created to protect systems against potential attacks. Be aware that attacks sometimes occur before updates are released. Make sure you update any software you use for browsing the Internet (Internet Explorer, Firefox, Netscape, Opera, Amaya, etc.) because Internet-based browsing attacks are becoming more common and more dangerous. Other software programs that communicate or interact with the Internet, like e-mail, Web servers, and remote desktop software are especially susceptible to attacks and should be kept current on patches and version levels.

3. Passwords and authentication methods.



Passwords and other authentication methods are ways systems verify that you are who you claim to be. If someone authenticates as you, the system will think it's you. That person can do anything you can do on your computer and the system will log their actions (such as deleting files, sending malicious e-mails, or browsing to inappropriate sites) under your access credentials. Don't share your passwords and access codes, don't store them in unencrypted files, and don't write them down unless you then place them in a

locked, secured location. Default passwords, names, and dictionary words, even in different languages, can be easily guessed or cracked so use complex passwords that are at least eight characters long and have numbers, letters, and special characters in them. Passwords aren't much use if you cannot remember them, so use a pass-phrase instead. The phrase "Would you like 3 scoops of ice cream?" can become the strong password "Wu13\$01c?"

4. Lock your workstation/laptop when you leave it and configure it to automatically lock after a short period of inactivity.

One of the fastest ways to compromise a system is to simply walk up to an unattended, unlocked workstation or server and access the system so be safe and lock your system when you leave it. It's also very easy to get sidetracked and stay away from your desk longer than you anticipate so configure your system to automatically lock after a short period of inactivity. It is an easy way to help protect your account and the items you have access to. Lockout after fifteen minutes of inactivity is recommended and shorter periods for critical systems.



5. Back up important files regularly.

There are many ways you can lose information on a computer – a destructive virus, a power surge, lightning, floods, a big magnet, or sometimes equipment just fails. If you regularly make backup copies of your files and keep them in a separate place, you can recover some, or even all, of your information in the event something happens to the originals on your computer. On-line back-up services are available or you can back up regularly to a system server, a CD, or a jump drive. Be sure to save physical back-up systems in a secure location if the information is sensitive or confidential. You might even consider a secure off-site storage location to protect against total building loss by fire.

6. Be cautious when using the Internet.



Browsing to non-work related sites can increase the risk of becoming infected with spyware, viruses, and other malicious code. Download files and install programs only when you are authorized to do so, and only when there is a real need. Know with whom you are dealing on the Internet – anonymous doesn't necessarily mean safe, and many criminals are very good at impersonating real financial organizations like banks and credit card companies. Never share personal or

confidential information if you are not the initiator of the transaction. Never share sensitive or confidential information over an unencrypted Internet connection.

7. Messaging security – e-mail and instant messaging.

E-mail and instant messaging (IM) are wonderful tools but they can be used or misused in a variety of ways. Do not send confidential or sensitive information, like Social Security numbers, account numbers, or secret information through unencrypted e-mail or IM. Do not open a message or an attachment from an unknown sender. If you share personal information with others as a result of answering spam or phishing messages, your identity can also be stolen.

8. Review your computer security.

Evaluate your computer's security periodically and apply appropriate repairs, upgrades, and replacements. If you don't maintain your system's security by keeping it up-to-date, it will eventually be exposed to serious security threats.

9. Responding to a cyber incident.

Learn how to recognize cyber attacks and know what to do if things go wrong. Ask if your organization has a cyber security incident response plan and a cyber security incident response team and use it when appropriate. Remember that rapid response can be crucial, so when things do go wrong or you encounter a suspicious security-related event, report it immediately. If you don't know how to report a cyber incident, ask someone in your IT department or your help desk.

10. Remember that cyber security is everyone's responsibility.

Just like one leak can sink a boat, one data leak, one security breach, or one malicious worm can sink an organization. By protecting yourself and the systems entrusted to you, you are protecting your co-workers, your entire organization's network and data and, ultimately, the citizens who are depending on you.

What are the risks?

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases or even worse, stealing your identity. Unfortunately, there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.



What can you do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).

Malicious code - Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the following characteristics:

- It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.
- Some forms propagate without user intervention and typically start by exploiting software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate via email, websites, or network-based software.
- Some malicious code claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

Viruses and worms are examples of malicious code.

Vulnerability - In most cases, vulnerabilities are caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities.

Portions of the preceding Cyber Security information are from:

<http://www.msisac.org> and <http://www.colorado.gov/cybersecurity>

Visit these sites for more information.

## File and E-Mail Management



An electronic mail message or “e-mail” is a digitally stored message and any attached digital documents transferred between computer users. State and local governments use e-mail for a variety of tasks such as sending and receiving internal and external correspondence, distributing memos, transferring official documents, and supporting various business processes and operations of the organization. Establishing policies, applying records management procedures, and training users can create an environment that promotes successful management of e-mail records.

The following tips and e-mail tools from *PC World* can help board members and staff manage e-mail overload.

- Set up folders to organize mail. Set up an "urgent" folder for top priority tasks; an "aging" folder for mail older than 30 days; and put all "cc" messages into a folder that doesn't require action. You might also create folders for tasks, and one for messages tied to upcoming events that don't require immediate answers. Beyond that, sort messages automatically by sender and date.
- Filter junk e-mail into the Delete folder--a clue is a subject line offering "one-time opportunity." Scan its contents occasionally to be sure you don't miss something useful.
- See if your e-mail program lets you view the first few lines in a message as well as the subject line; it might be enough to handle the message.
- Rely on integrated group-scheduling programs such as Exchange, GroupWise, and Lotus Notes to automatically update your calendar.
- Write boilerplate text to answer common e-mail inquiries, and consider automatic replies as well. Increasingly sophisticated software can read e-mail, categorize it, refer it, and prepare draft replies.
- Subscribe to mail lists sparingly.
- Maintain separate personal and business e-mail accounts.

### Break Backlog Behavior

- Changing your habits also eases e-mail pressure. Set a time in both the morning and afternoon to handle e-mail, and deal with each message only once.
- Etiquette also applies to e-mail, the researchers say--and you may spread good habits by example: Don't overwhelm a colleague's mailbox with large attachments that slow down or overwhelm e-mail systems. Graphics--such as pictures-- typically can be very large even if only one picture. Changing files to pdf (if they can be read-only) or “zipping” files can significantly reduce their size. If you are sending information from a shared source such as the web, send the link to the site rather than attach the actual document whenever possible. Write clear, succinct subject headers, which help to sort mail. For that matter, write clear, succinct messages. Don't label a message "high priority" unduly, and use cc: sparingly. Avoid chain letters and jokes. Remember, not every e-mail requires an answer.
- Businesses can force the issue by setting e-mail policy about acceptable size, style, and use of mailing lists (or spam).
- The e-mail challenge continues to grow. Besides getting digital messages on your PC, you'll get them on pagers, handhelds, and cell phones. Also, experts expect spam will occupy 40 percent of your mailbox in the future. But the researchers also foresee

additional tools to help us deal with them. A single mailbox could collect e-mail from those numerous sources. Tools to automatically sort e-mail will become more sophisticated, and you'll have more ways to take out the digital trash.

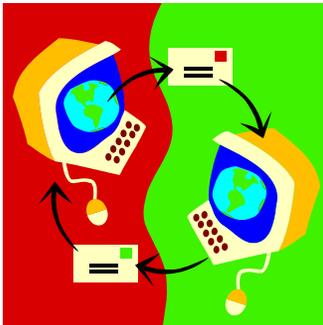
## NRCS Computer Security Requirements

Federal guidelines require that district employees undergo background investigations and credit checks in order to use federal computers.

- These requirements are based on a federal government-wide directive. All government partners, contractors, and others who have access to government computers must comply. Districts employees are not being singled out and unfortunately this type of extra precaution is felt to be necessary.
- The credit check is a basic requirement of the federal government and many private businesses. USDA is only interested in the identity portion of the report and not the credit information.
- Each state is handling the payment of the back-ground requirements differently and each state conservationist does have the flexibility to help defer a portion or all of the costs if their own state budget allows. Districts should enter into an agreement with NRCS state offices regarding the collection and/or payment of fees. NACD encourages districts to work with their state NRCS office to work out these details. Fortunately in Colorado, NRCS covers all the costs associated with the background and credit checks.
- USDA can only accept OPM as the valid source for background investigations, so background investigations conducted by state, local, or private agencies are not valid for these purposes.



## What to Forward to the Board



It is often difficult to determine what information to forward to the Board. This process should be discussed with the Board so that both the district employee and the Board are clear on what information is considered vital and must be handled with urgency due to time-sensitive issues. Establishment of e-mail and communication policies is important in the day-to-day operations of the district, including identifying the method of forwarding communications to the Board. Hopefully most board members have access to e-mail as an effective, inexpensive, convenient, and most importantly, timely method to disseminate important information to board members in the current digital environment.

Some boards may want more information forwarded than others, or forwarded more or less broadly to board members. It really is a district-by-district decision and requires good judgment by the district manager in implementing the forwarding policy. It is important to strike a balance between sufficient and effective communication and overwhelming board members so that forwarded information tends to be overlooked.

Forwarding to the board typically has one of three objectives:

1. To ensure rapid response to a time-sensitive issue
2. To provide information prior to a meeting for individual review
3. To provide electronic information to the board instead of hard copies delivered at a board meeting.