Keep

DHS

Security
Awareness
F or
E veryone

Georgia Department of Human Services
http://DHS.georgia.gov/portal/site/DHS/

This information was provided by the DHS Information Security Office Please send any questions, comments, or to report any Information Security related incidents to:
infosec@dhr.state.ga.us

Acknowledgement

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative effort for State and Local Governments in strong partnership with the US Department of Homeland Security.

Georgia Department of Human Services
Office of Information Technology
Information Security
2 Peachtree Street, NW 4th Floor
Atlanta, Georgia 30303
InfoSec@dhr.state.ga.us
DHS Helpdesk 1-800-764-1017
@2005 Multi-State Information Sharing & Analysis Center (MS-ISAC)

October 2007

Georgia Department of Human Services
Office of Information Technology

Information Security Awareness

The Goals of Information Security are:

- **Confidentiality** - Protecting sensitive information from unauthorized disclosure.
- **Integrity** – Ensuring information is authentic and not corrupted.
- **Availability** - Ensuring information is available when needed.

FASTER. FRIENDLIER. EASIER.

Georgia

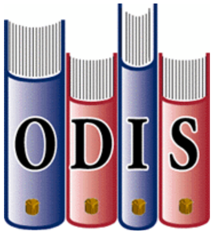
Introduction

Information is a critical asset. Therefore, it must be protected from unauthorized modification, destruction and disclosure. This pamphlet describes information security concepts and defines steps required to properly safeguard information. It is the responsibility of everyone—each employee and resource user— to become familiar with good security principles and to put them into practice when working with State-owned information.

Did You Know?

Based on recent statistics:
That the average unprotected computer can be compromised in a matter of minutes.

The majority of individuals who thought their computers were safe were wrong.



DHS Information Security Policy, Standards & Guidelines

Online Directives Information System **(ODIS)**
HTTP://www.odis.dhr.state.ga.us/

Click Index
Click Administration
Click Information Technology
Click POL1900 for the Information Security Policy Directive
Click MAN1900 for the Table of Contents (TOC)
Click Open
If MAN1900 is chosen, click on desired document in TOC

Human Services Personnel Policy #1205
http://www.odis.dhr.state.ga.us/1000_adm/1300_ohrmd/Manual/1205.pdf

Security Breaches

Security breaches can take several forms. The best defense against security breaches are conscientious and alert users. You are the most important person for early detection and prevention. Examples include:

- Damage to equipment, facilities or utilities.
- Loss or misplacement of media (e.g. disks, tapes, paper) containing confidential/highly restricted information.
- Unauthorized access or attempted unauthorized access to information or computing resources.

If you discover a security breach, you should report it immediately to the Information Security Team Office at **infosec@dhr.state.ga.us.**

Shred it and Forget it

We are required to properly dispose of data that is of no more use, regardless of the media type.

- Overwrite—DOD Standard 5220.22-M
- Degauss—Electromagnetic cleansing
- Destroy—Physical destruction of the media

At The End of The Day

- Perform a perimeter check at the end of the day
- Lock away papers containing sensitive information
- Shut down your computer
- Click Start. . .select shut down
- Make sure no sensitive information

E-mail Etiquette

- Keep your mailbox clean, delete unnecessary e-mail and create folders for the rest.
- Limit the size of attachments and save attachments off the system.
- Do not attempt to send files with **.exe, .bat, .com, .pif,** or **.scr** these are common methods of virus infection.

Possible Symptoms of a Compromised Computer

Is your machine:

- Slow or non-responsive? Experiencing unexpected behavior?
- Running programs that you weren't expecting?
- Showing signs of high level of activity to the hard drive that is not the result of anything you initiated?
- Displaying messages on your screen that you haven't seen before?
- Unable to run a program because you don't have enough memory – and this hasn't happened before?
- Program constantly crashing?
- Rejecting a valid and correctly entered password?
- Finding there are new or anonymous processes running on the machines?

Call the DHS Helpdesk **1-800-764-1017** for immediate assistance. For questions regarding incident reporting, email the Information Security Team at infosec@dhr.state.ga.us. Home users may wish to contact their ISP and/or anti-virus vendor.

User IDs and Passwords

Your user ID is your identification, and is what links you to your actions on the system. Your password authenticates your user ID. Protect your ID and password. Remember, you are ultimately responsible for actions taken with your ID and password.

Follow these best practices:

- Your password should be changed every 30 days.
- Don't reuse your previous passwords.
- **NEVER** tell or share your password with ANYONE.
- **NEVER** write your password down anywhere—the downfall of a network could be that yellow post it note under your keyboard with your password on it.
- If your computer prompts you to save your password, click "**No**."
- Use DHS Guidelines and choose a strong password:
- Be sure your password is at least eight characters long.
- Be sure it contains uppercase & lowercase letters, at least one number and at least one special character (!@#$%&*).
- Do not use personal information like names, birth dates, children's names, etc to create passwords
- It should not be easily guessed, but easy to remember.
- If you have difficulty in thinking of a password that you can remember, try using the first letter of each word in a phrase, song, quote or sentence. For example, "The big Red fox jumped over the Fence to get the hen?" becomes TbRfjotF2gth?.
- If you think your password has been compromised, change it immediately. Employees should notify the information security officer or manager at their organization of any suspected or known compromise.

Computer Protection

Properly safeguarding your personal computer (PC) is one of the most important ways of protecting your information from corruption or loss.

Lock your computer when you are away from your desk. Press

“Control, Alt, &Delete” keys simultaneously, and then click “Lock Computer” to lock. You will need your password to sign back in, but doing this several times a day will help you to remember your password.

Protecting your Information

1. During an emergency or disruption, critical information— the information necessary to run DHS’s systems, record activities or satisfy legal and/or business requirements— may be damaged. The best way to protect information is to copy it and store it in a secure location.
2. If you are connected to a network, store your files in folders created for you. (For employees, check with your LAN administrator for the schedule of backups).
3. If you are not connected to the network, save your files to appropriate storage media and secure them properly.
4. Ensure that backups reflect the most current information by copying the data on a regular basis, and after any significant changes. The frequency of the backup cycle should be consistent with the frequency with which you modify the information.

Internet Usage

DHS staff should use the Internet to accomplish job responsibilities more effectively and to enrich their performance skills.

- Internet access is provided to facilitate State Business.
- Internet access is monitored and recorded.
- Each use of the internet must be able to withstand public scrutiny without embarrassment to DHS or the State of Georgia.
- Users must not access inappropriate sites (i.e. Illegal activities, wagering or betting. receipt, storage or transmission of offensive, racist, sexist, obscene or pornographic information, etc.)

Wireless Security

Wireless networks and laptops are very popular for their ease of use and portability. The Internet can be reached via radio waves without having to plug your machine into a network. It is with the same ease of connecting that malicious individuals connect to unprotected networks. Attackers conduct drive-by eavesdropping, called “war driving” to listen in on unsecured devices in homes and businesses.

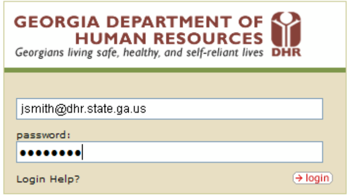
- Change the default passwords and default SSID. Most default passwords are known to hackers.
- Turn off broadcasting the SSID if possible; this will make it more difficult for a hacker to gather your SSID information.
- Turn on encryption - Encryption settings should be set for the strongest encryption available in the product.
- Change the default cryptographic key - Many vendors use identical shared keys in their factory settings.
- Use MAC ACL filtering - The MAC Access Control List (ACL) can permit certain MAC addresses access to the network while denying access to other MAC addresses, limiting access to only authorized computers.
- Please follow DHS policy regarding the use of DHS Information Technology Resources.

DHS Employee Intranet Login

https://intranet.dhr.state.ga.us

Q. How do I login to the DHS Employee Intranet?
A. Login using your GroupWise e-mail address and your Novell NetWare password (the one you use to login to your PC every morning.

(Example: jsmith@dhr.state.ga.us.
And use your Novell password, NOT your GroupWise password.)



GEORGIA DEPARTMENT OF HUMAN RESOURCES
Georgians living safe, healthy, and self-reliant lives DHR

jsmith@dhr.state.ga.us

password:
••••••••

Login Help?

Mobile Computing Security

Computers are now accessible via a variety of means. A person can even download data from the Internet to a cell phone. While convenient and fun to use, some good practices will help protect your information.

Laptops, PDAs, Blackberry's and Cell Phones are more easily stolen or misplaced because of their size. Remember, if your laptop is gone, your data is too. Small computer devices carry information that must be protected. Enabling security features is a recommended practice.

If you use a mobile device please remember the following:

- Secure it with a cable lock or store it in a locked area or locked drawer.
- Backup your data.
- Password protect it.
- Encrypt confidential information stored on it.
- Keep it with you during air and vehicle travel until it can be locked up safely. Do not forget to retrieve it after passing through airport security.

Treat all your portable devices in the same careful manner as your laptop and keep an eye on them.

Personal Equipment

Users are prohibited from attaching their personal computers, laptops, handheld devices to the network without written consent. Doing so could potentially infect our environment and cause a disruption of services to the constituents of Georgia. DHS reserves the right to search PCs and remove

Remote Access allows users to access data from outside of the DHS network. Because this form of access is designed for off-site use that may extend after normal business hours, extra measures are required to prevent unauthorized access.

- Remote access to the office via the Internet should use encryption such as Secure Socket Layer (SSL) or Virtual Private Network (VPN).
- All policies regarding the use of DHS resources extend to remote locations.

GroupWise Access via the Internet

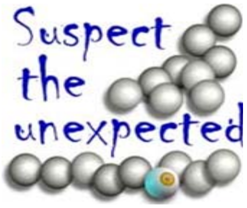
Availability to GroupWise from home or away from the office:

- Type the following in your browser address line: http://gw.dhr.state.ga.us
- Please select one of the three GroupWise servers.

For additional help with GroupWise, click on Help at the main GroupWise Web Access page or go to http://gw.dhr.state.ga.us/faq/

E-mail Usage

Email represents the most common method for the spread of malicious programs. Confidential information can very easily be accidentally and/or purposefully compromised via email. Employees are expected to conduct their use of email with the same integrity as in face-to-face or telephone business operations.



Malicious Code Protection

Malicious code can take forms such as a virus, worm or Trojan. It can hide behind an infected web page or disguise itself in a downloadable game, screen saver or email attachment.

Don't Open Unexpected Email

Computer viruses are programs that spread or self-replicate. They usually require interaction from someone to be activated. The virus may arrive in an email message as an attachment or be activated by simply opening a message or visiting a malicious web site. Some viruses consume storage space or simply cause unusual screen displays. Others destroy information. If a virus infects your PC, all the information on your hard drive may be lost and/or compromised. Also, a virus in your PC may easily spread to other machines that share the information you access.

Viruses can exhibit many different symptoms. If your computer behaves erratically, employees are advised to contact the DHS Helpdesk at **1-800-764-1017.**

Malicious Code Protection *(Continued)*

Anti-virus software is updated regularly on DHS owned machines via automatic updates. New, fast spreading worms and viruses are released every day.

Store removable media, such as CDs, thumb drives, and diskettes as "write protected" whenever possible to help prevent infection by viruses.

Worms are similar to viruses because they self–replicate, however, they do not require any user interaction to be activated. Worms spread because of vulnerabilities or “holes” in software.

Trojans (also known as backdoors) are malicious code hidden in a legitimate program that, when executed, perform some unauthorized activity or function. This can range from stealing your password and credit card information to allowing someone to take control of your computer.

A **denial-of-service attack** is an assault upon a network or web site that floods it with so many additional requests that regular services are either slow or completely interrupted. In some instances, a group of remotely controlled, compromised desktops are combined to jointly attack a target system.

Spyware and related “adware,” are software sometimes downloaded from a web page, by clicking on a link in an email. It is also installed with freeware or shareware software without the user’s knowledge. Spyware is used to track your Internet activity, redirect your browser to certain web sites or monitor sites you visit. Spyware may also record your passwords and personal information to send to a malicious web site.

- Choose to “*Close*” any pop up windows by clicking on the “*X*.”
- Do not respond to any dialogue boxes that appear unexpectedly; click on “*X*”, in the upper right corner of the dialog box. Clicking on “*No*” or “*Cancel*” inside the dialog box sometimes installs spyware.
- Beware of web sites that are un-trusted.

Hoaxes are e-mail messages that resemble chain letters, offer free money, or contain dire warnings and offers that seem to be too good to be true. If you receive a hoax via email, delete it. Sharing hoaxes slows down mail servers and may be a cover for a hidden virus or worm.

Chain Letters cover any variety of topics including anything from spiders in the toilet to free gift certificates or even getting paid to forward email. Chain letters create a high volume of mail. If one person forwards 1 message to 10 people, by the sixth generation, you will have over 1 million messages. Remember, at DHS alone we have over 9,000 employees. That type of volume could potentially take down the entire mail system here, not to mention the damage it could do outside of DHS.

Phishing is a scam in which an email message directs the email recipient to click on a link that takes them to a web site where they are prompted for personal information such as a pin number, social security number, bank account number or credit card number. Both the link and web site may closely resemble an authentic web site however, they are not legitimate. If the phishing scam is successful, personal accounts may be accessed. If you receive one of these emails:

- Do not click on the link. In some cases, doing so may cause malicious software to be downloaded to your computer.
- Delete the email message.

Do not provide any personal information in response to any email if you are not the initiator of the request.

Just say NO!