



GEORGIA DEPARTMENT OF
COMMUNITY HEALTH

Secure Computing 101



Office of Information Technology



Network and Information Security starts with you

The IT department uses the latest technology and techniques to maintain the highest level of security possible, but we can't do the job without your help.

Every employee is responsible and plays a critical role in keeping DCH's computer network secure.

When you log on to your computer, send an e-mail, share a file, or access the internet, you can help or hurt network security.



Why bother with security?

- Policy Requirements:
 - State of Georgia IT Security Policies
 - DCH Information Security Policies
 - HIPAA Compliance



Why bother with security?

- Hackers and viruses can destroy your work.
- Private information can be compromised.
- Your ability to work can be hampered.



What Makes Us Vulnerable?

- **Easily guessed passwords** – Too short; too simple; common words
- **Not keeping secrets** – Writing passwords down; posting it on monitor or under keyboard.
- **Sharing user ids and passwords** – allowing someone else to logon as you.



Password Security

- **Don't** tell anyone your password.
- **Don't** write your password down anywhere.
- Make sure your password cannot be easily guessed and is not personal information.
- If you think there is even a slight chance someone knows your password, change it.
- **Don't** let someone see what you are entering as your password.



Do Choose a **Strong** Password:

- That is at least eight characters long.
- That contains uppercase and lowercase letters.
- That contains at least one number and/or special character.
- That is not personal information like names, birthdates, children's names, etc.
- That cannot be easily guessed and is easy to remember.
- Remember to change your password every 30 days.



INTERNET USAGE

- 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 DCH or the State of Georgia.
- Limited personal use is acceptable and is subject to the same acceptable usage policies.
- Users must not access sites deemed inappropriate.



Inappropriate Internet Usage

- Illegal activities
- Wagering or betting
- Harassment and illegal discrimination
- Commercial activities (e.g., personal for-profit business activities)
- Promotion of political or religious positions or activities
- Receipt, storage or transmission of offensive, racist, sexist, obscene or pornographic information
- Downloading software (including games, wallpaper, weather programs and screen savers) unless agency sanctioned (and installed by DCH Technical Support).
- Use by individuals other than state employees
- Chat sessions or bulletin boards, unless business related.
- Web based/non-dch email, chat or messenger accounts (hotmail, yahoo mail, etc)



GEORGIA DEPARTMENT OF
COMMUNITY HEALTH

ACCESS PENDING/DENIED

**The site requested MAY be inappropriate
for State Business.**

**If you feel this is an error, please email
the site address info to Network Security**

[Click here](#)

Follow the instructions below if you would like to request that a website is unblocked for business purposes:

- Copy the address from the address line
- Click on the Click Here link.
- Paste the address into the email and send.

Your request will be reviewed for release.



E-mail

- E-mail represents our single biggest security concern.
- Viruses are most commonly spread through e-mail attachments.
- Confidential information can very easily be accidentally and/or purposefully compromised through e-mail.
- Employees are expected to conduct their use of email with the same integrity as in face-to-face or telephone business operations.



Email Threats

- ***Spoofed email:*** Looks as if it came from one user but originated somewhere else.
- ***Zombie machines:*** Infected machines across the internet responsible for sending thousands of spam and infected email without the user being aware of it.
- ***Phishing Scams:*** Emails that may look like official bank correspondence requesting you to verify your personal information. Your bank will never request information in that manner.
- ***Chain letters and hoaxes:*** Don't respond to them and don't resend them to 10 of your friends. I'm willing to bet that you won't grow feathers if you don't.
- ***Malicious Internet links in email:*** Users click on internet links in emails that redirect them to infected sites or sites that install malicious software on user machines.



Viruses and malicious programs can come from:

- E-mail attachments.
- Internet sites and software downloaded from the Internet.
- Infected files shared via removable storage (diskettes, CDs, Zip disks, and other media) or over the network.



Here is what you should do:

- Do not open unexpected e-mail with/or without attachments, even from coworkers or other trusted sources...use Shift Delete
- Never open attachments from an unknown or suspicious source...use Shift Delete
- Do not reply to or attempt to unsubscribe from spam messages. This just verifies a valid email address...use Shift Delete
- Never download freeware or shareware or install software or games from disks brought in. If you have a business need for a particular program, contact the help desk and a technician will be assigned.
- Understand that any e-mail message sent over the Internet could possibly be read by others. Email is not SECURE.
- Remember email has been provided for business purposes. DCH owns all incoming and outgoing e-mail messages.



Email Housekeeping

- Mailboxes have a limit of 100mb of space. You will receive a warning when you are close to the limit. If you reach your limit, you will not be able to send or receive email. Contact the helpdesk for instructions or assistance on cleaning your mailbox.
- Email attachments cannot be over 5mb. If there is a business need to send a larger file, use Winzip to reduce the size, or contact the help desk for additional transmission options.
- Email is subject to certain blocking filters:
 - Subject
 - File Extension
 - Filenames
 - Embedded Websites
 - Sexual Content

Any email that fits the criteria will be blocked.

It is recommended that you review the `blockedlist.pdf` file located in `o:\common`.



Reporting Computer Security Incidents

- If you believe someone has stolen your password or illicitly accessed your computer, call the help desk.
- If you forget your password or need to have a temporary account created, call the help desk.
- If you receive a suspicious e-mail, call the help desk for instructions.
- If you put infected media into your computer, the anti-virus software will ask you to eject, scan or format the disk. Eject the disk and contact the help desk or network security.
- All media should be scanned before use.
- If an infected file is critical, the IT department will attempt to rescue the data. Success is not guaranteed.



End of Day Procedures

Logging OFF Workstation

- Close all open programs by clicking the **X** in the upper right-hand corner of each application
- Click the **Start** button in the lower left-hand corner and select the **Shut Down** button
- Select **Restart** from the drop down menu and click **OK**

.



FAQ

What if I can't log on?	Contact the Help Desk.
What if I can't get into the e-mail system?	Contact the Help Desk.
What if I forget my new password and get locked out of the system?	Contact the Help Desk. We will reset your password, and you will have to create a new one the next time you log on.
Should I turn off my computer before I leave work?	Unless otherwise instructed by the Help Desk, no. Always leave your computer on. Before you leave work, log off the system but leave the computer turned on.
Should I ever lock my workstation?	Yes. You should lock your workstation any time you leave your desk for more than five minutes.
What if I can't print?	Check to ensure that you've selected the correct printer. Check the printer for any noticeable problems (low toner, paper jam, etc.). Contact the Help Desk.
I think my machine is infected with something.	Contact the Help Desk IMMEDIATELY.
What if I need additional software installed on my computer?	Contact the Help Desk. If there is a business need for the installation, a Technician will be assigned.
What if I need to move my computer to another location?	Contact the Help Desk. All computer, network, telecommunications, or presentation equipment moves should be handled by the Help Desk.



How to contact the Help Desk

1. Telephone

- Ext. 7-7171 from any DCH telephone
- (404) 657-7171 local

2. E-mail

- **To:** Help Desk
Subject: Brief problem description
Body: Detailed problem description including: location of the problem, number of people affected, severity of problem, and contact information.

3. In Person

- **38th Floor, Northwest corner**

*****Do not contact Technicians directly*****

Questions???

