Office of the Mayor
City of Columbus
Ohio

LAPTOP POLICY

Overview

Laptop computers and other Mobile information assets (Blackberries, Tablet PCs, Personal Digital Assistants (PDAs), etc.) make it possible for City employees to support Columbus citizens anywhere, anytime. However, mobile computing increases the risk to the City because they are more vulnerable to loss and theft.

This policy builds on Executive Order 2007-03, which addresses laptops and sensitive information. It incorporates relevant information from the greater City of Columbus Security Policy published by the Enterprise Security Risk Management (ESRM) group.

Your Department's policy on the subject takes precedence.

Purchasing A Laptop

The first question you should consider is whether you need a laptop in the first place:

1. Will you need a laptop all the time? (You should consider using a laptop shared by other employees in your Department.)
2. Do you just need to check e-mail from home? (Did you know you can check e-mail using the City's Outlook Web Access site?)
3. Do you need to check e-mail away from your office and home? (A Blackberry may be all you need.)

Once you have decided you need a laptop, you must purchase it through the City's established channels regardless of the source of funding (grant, UTC, seizure funds, donation, etc.). It must adhere to the Department of Technology's (DoT) hardware standards. Otherwise, it may not work properly with the protection software installed and you will not be permitted to connect to the City's network (MetroNet).

Physical Security Controls For Laptops

The physical security of *your* laptop is your personal responsibility, so please take all reasonable precautions:

1. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag, or mobile phone. Be extra careful in public places such as airports, railway stations, or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
2. Never leave a laptop visible in an unattended vehicle. If it is absolutely necessary to do so, lock it out of sight in the trunk. Remember, it is much safer to take it with you.
3. If you have to leave the laptop unattended in your office, meeting room, or hotel room (even for a short while), use the laptop security cable you were issued to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.
4. When you are not using the laptop, store it out of sight preferably in a safe, a lockable drawer, or cabinet. This applies at home, in the office, in a hotel, etc.
5. If your laptop is lost or stolen, call (614) 645-5758 (DoT Service Desk) as soon as possible. This phone number (monitored 24 hours a day) will alert security personnel of the event. They will contact you to gather detailed information such as the sensitivity of the information stored, how it was protected, etc.

6. Based on their assessment, they will initiate the Incident Response (IR) process. Response includes notification and escalation to your department, the Mayor's Office, law enforcement officials, etc. depending on the severity of the incident. (Note: a Security Hotline is currently under development to enhance the City's IR effectiveness).

Unauthorized Access To Information On Laptops

If you are authorized through your Department to store sensitive information on your laptop, it must be protected with DoT-approved encryption software. This type of software provides extremely strong protection against unauthorized access to the data in the event your laptop is lost or stolen.

While your laptop's Operating System (OS) will require your password meets the City's security policy requirements, you can defeat this layer of protection by writing down or sharing your password. Remember you are personally accountable for all network and systems access under your user ID.

When using your laptop:

1. Your work must be directly related to City business.
2. Never connect directly to the Internet. You must first connect to MetroNet ("VPN-in," log in using Terminal Services, etc.) and access the Internet through it like you would do from your office. This will ensure the information stored on it is protected from Internet-related threats by MetroNet's built-in protection
3. Never leave it unattended or "unlocked." This will prevent anyone from viewing information, or accessing it using your User ID and password. Always shut down, log off, or activate the password-protected screensaver before stepping away from it.

Malicious Code Protection

Malicious code (viruses, worms, Trojan horses, spyware, etc.) is a threat to the City's information assets. Laptops are particularly vulnerable because you may not log on to the City's network for extended periods of time.

Please log into MetroNet at least monthly. Protection software is automatically updated only when the laptop is connected to the network. If you cannot log in for any reason, contact the Service Desk for advice on how to obtain and install protection software updates.

Additional precautions you must take when using your laptop include:

1. Not opening e-mail attachments unless you expect to receive e-mail from the sender.
2. Promptly report to the Service Desk any alerts or signs (unusual behavior or file activity) indicating your laptop has been exposed to malicious code. This will minimize the impact to the information stored on it.