

PROTECTING PORTABLE COMPUTING AND STORAGE

University of Miami Ethics Programs

WHY WORRY ABOUT PORTABLES?

- **Vulnerable to accidental loss and damage** – Offices are relatively safe places. Unfortunately, portables don't usually stay in the office.
- **Vulnerable to theft** – Portables are also attractive targets for thieves, and it can take only seconds to steal one. (They're not just portable for you.)
- **Contain lots of information** – Portable devices can store huge quantities of data. That makes their loss potentially a disaster.

The expression in information security is "appropriate defense in depth." While better than nothing, one type of protection strategy is rarely enough. But it is equally rare to need all the protections we list here. Unfortunately, there is no rule about how much security is needed for a portable. It depends on the vulnerability of the device, given how you use it, and the sensitivity of the information on it. If you're not sure what's appropriate for your circumstances, ask someone in your security department.

SUGGESTIONS FOR PROTECTING PORTABLES

- **Keep it in physically secure spaces** – The most important defense for your portable is a secure physical space, like a protected office environment. Taking a portable out in the world is always risky. Millions of insurance claims each year for damaged, lost or stolen computers are the proof.
- **Always assess the environment** – The reason you have a portable is so you can take it with you. When you do, always be aware of the security of the new environment into which you take it.
- **Apply the Ben Franklin Test** – Not sure about the environment? If you wouldn't leave a \$100 bill unattended in a particular place, you probably shouldn't leave your portable there either.
- **Attend to secure storage and transit** – When it's not in use, keep it locked up. On the road, keep it close – and when you can't, keep it as locked up as possible, and as hidden as possible.
- **Protect it with locks and alarms** – Physical locks and alarm devices are relatively cheap and can provide a measure of protection in an otherwise insecure physical space.
- **Protect it with labels and engraving** – Permanent labels and/or engraving can facilitate return of a lost device, and make it a less attractive target for theft.
- **Protect it with passwords** – If you keep sensitive information on a portable (and who doesn't?) passwords and other access protections should be used whenever the portable device allows it.
- **Protect it with encryption** – Encryption tools can provide a virtually impenetrable barrier for particularly sensitive data on a portable. But at the price of some inconvenience.

- **Protect it with tracking systems** – Tracking software can be installed to report a stolen portable's location when it uses the Internet; some systems also provide the capability for remote file deletion. This is not a cheap solution, but it may be appropriate for particularly sensitive data.
- **Attend to communications security** – A portable device is often a wireless device. If your portable has Wi-Fi/Airport (802.11) and/or Bluetooth capabilities, be sure they're configured securely. If you're accessing sensitive data from off-site, attend to secure end-to-end communications too.
- **Minimize sensitive data storage** – The less sensitive data you keep on a portable, the less you need to worry about sensitive data exposure if the device is lost or stolen.
- **Maximize password safety** – If you use passwords, pick good ones. And keep them secure. (While we're on the subject, if you use your portable to surf to password-protected web sites, it's generally a bad idea to use the "remember my password" option.)
- **Keep secure backup copies** – At least you'll have access to your data again if you keep secure backup copies of all the data on a portable.
- **Secure disposal** – Be sure you dispose of those backup copies, and the device itself, in a secure way when it's no longer needed.
- **Reporting losses** – Be sure to report the loss of any sensitive data to appropriate authorities in your organization. Make a report even if the device is recovered. The confidentiality of the information may have been compromised while the device was out of your control.
- **Security on "borrowed" systems** – If you do decide to rely on others' computers, rather than toting yours around, be aware of the security perils of borrowed systems. You can leave a lot of sensitive information behind.
- **Loss and damage vs. theft** – When theft is always a worry, given the attractiveness of portables to thieves, accidental damage and simple loss are much more likely. Make sure your security steps take all the risks into account.

► *Questions and comments about this document are welcome. Send email to ethics@miami.edu.*