Mobile Computing Standards

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mat_060106_cd44

Information System Security
Mobile Computing Standards and Guidelines
for Users

When traveling or outside a secure environment, the security risk to your laptop or PDA and the data it contains increases. Loss, theft, and interception of data are more likely to occur when you are using your mobile device in an non-secure environment such as a mall, airport, restaurant or other public space. This document provides guidelines to help you avoid a security incident.

Possible security incidents that you can encounter while traveling or outside a secure environment are:

- When trying to keep travel schedules, it is all too easy for you to put your laptop or PDA down and forget about it. By the time you realize what has happened, it is too late—your laptop or PDA is gone and so is your data.
- Thieves target laptops or PDAs because they are portable and highly valuable. They may also target them because of the data they contain. If an enterprising thief discovers that you work for USAID, he or she may target your laptop or PDA knowing that it contains valuable information.
- Using your laptop or PDA in a public place creates an opportunity for thieves to directly observe you while you are working.
- While using a wireless or hotel network, your connection could be monitored or your system could be compromised. These networks, while convenient, provide little or no protection against thieves intercepting or capturing your data.

Protect your laptop or PDA and the data it contains by following these guidelines:

- You must use passwords that meet or exceed the USAID password standards.
- You should encrypt, using CISO-approved encryption, any information that you store on a laptop or PDA. In some cases the ISSO may **require** that you do so.
- You should make backups of your data and carry them separate from your laptop or PDA.
- If you connect to any USAID network, then you should not simultaneously connect to another network. The only exception to this standard is when you use an CISO-approved remote access solution (i.e. the second network is a pass-through to the USAID network).

- You should not store personal information into “profile assistant” programs, browsers, Windows operating systems, etc. Personal information includes full name, phone number, address, credit card number.
- You must not check your laptop or PDA as baggage. Carry it with you and keep it within reach.
- You must not leave your laptop or PDA unattended at any time while traveling.
- You must not place your laptop or PDA into a taxi trunk.
- If you leave your hotel room, you must keep your laptop or PDA with you or store it in a secure area in the Mission you are visiting.
- You must not allow any hotel staff member to carry your laptop or PDA.
- You must not use your computer to process SBU information while in transit, or in “open environments” such as lobbies, restaurants or other public places.
- You must use a CISO-approved personal firewall on laptops.
- You must use CISO-approved anti-virus software on laptops.
- If you are not actively using your wireless LAN card, then you should disable it.