

# Dell Notebook Security

## Recommended Best Practices:

September 2007

The following areas should be addressed to help deliver optimal notebook PC security:

- 1) Security Audit Services
  - a. Dell Recommends the ISO 17799 Audit (SKU A1270104)
  - b. Dell also offers additional security professional services
- 2) HDD Encryption (Helps protect data if Notebook is stolen)
  - a. Dell Recommends the Dell HW Encrypting HDD with Wave's EMBASSY Trust Suite for Dell 3.0 Enterprise software (Legend Code 120DENW)
  - b. Dell Recommends managing HW encrypting HDD with Wave™ Systems Embassy Remote Administration Server (ERAS) SW (Deployment bundle SKU A1233138)
  - c. Dell also offers SW encryption solutions from Credant™, Pointsec™, Safeboot™, Utimaco™ and others.
- 3) File and Folder Encryption designed to protect files from being read by unauthorized users on the local HDD, when shared with others or stored on other devices like USB memory devices and enables E-mail encryption)
  - a. Dell recommends using the managed TPM based encryption solution from Wave Systems
  - b. Dell also offers other encryption solutions including e-mail content protection SW.
- 4) Dell BIOS Settings (allows administrators to configure a system to meet the security needs of the customer's environment.) Most customers should include the following settings:
  - a. Disable USB ports (or install port management SW )
  - b. Limit boot to the internal HDD
  - c. Enable Pre-boot authentication with a password or Smart Card
  - d. Lock the BIOS setup menu with a complex administrator password (that the user does not know)
- 5) Make sure that all SW and OS patches and updates have been installed
- 6) Install a robust Anti-Virus and Anti-Malware solution
- 7) Limit user OS privileges (do not give users OS administrator privileges; for example: do not allow users to load or remove SW applications)
- 8) Utilize Managed Strong Multi-factor user Authentication Solutions
  - a. Dell BIOS allows Smart Card pre-boot authentication credentials to be automatically passed to the operating system at boot time
  - b. Dell offers several Smart Card and Biometric solutions

9) Utilize Network Access Control (NAC) solutions (to help prevent systems that do not have up to date security configurations from connecting to the network)

10) Physical Locks

- a. Dell offers many varieties of custom locking solutions
- b. Custom keying and master key solutions are also available