



## Laptop Computer Security

**Introduction** Laptop computers are subject to all of the security vulnerabilities that threaten desktop computers. In addition significant threats arise from transporting it through uncontrolled settings and using it in high-risk IT environments. Laptops represent a growing proportion of all end-user computer platforms, most incorporate multiple network connection technologies, it is this inter-connectivity flexibility that renders the laptop more vulnerable to cyber threats. A Threat and & Analysis (TRA) is required to identify security vulnerabilities and determine the required security requirements.



**Life Cycle** Applying the TRA security requirements at every opportunity in the laptop's life cycle maximizes its defensive capability and reduces the risk that the device can be compromised.

**Working Environments** A laptop may be used as a 'desktop' replacement directly connected to the department's IT network, at home while connected directly to the user's ISP access portal and a VPN to the department's network or at another location using a publicly available wireless access point (Hotspot).

A laptop is a high value item highly susceptible to theft; never leave a laptop unattended in public; use disk encryption to protect the confidentiality of the department's data in the event that the laptop is lost or stolen.

A laptop is at high risk from network based threats while connected to a network 'hotspot'; utilize Firewall, IPS, IDS and secure user and network authentication to reduce the risk of network based attacks.

### Basic Security Recommendations

**Protection** – Never leave a laptop unattended in public and use physical locking cables to secure the device. Use disk, folder and/or file encryption to protect the data stored on the laptop.

**Patches and Updates** – Maintain the laptop computer: install the latest software updates and security patches.

**Connectivity** – Require VPN connectivity for remote department access. Disable all wireless connectivity not specifically required by the user. Use firewall, IPS and IDS technology to reduce the risk from cyber threats.

**User Privileges** – Provide user access rights based on 'least privilege'; the user account should not be an 'administrator'. If required provide the user a separate user-administrator account for remote problem resolution.

**Password Security** – Require secure user authentication. Change all default passwords.

**Printed Output** – Enable the private printing feature so that users must authenticate at the console in order to complete the print job.

| Risk                                | Mitigation  |
|-------------------------------------|---|
| Laptop<br>Loss / Theft              | <b>Physical Security:</b> Never leave a laptop unattended, use a physical locking device, use laptop tracking software, backup data to removable.   |
| Data<br>Integrity / Confidentiality | <b>Data Security:</b> Use strong login credentials, encrypt stored data, encrypt data in transit and encrypt wireless network traffic.              |
| Cyber Attack                        | <b>Cyber Security:</b> Require VPN connectivity to department network, Use Firewall, IPS and IDS tools, use wireless connectivity only if required. |