

UNCLASSIFIED



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

COTS SECURITY GUIDANCE (CSG)

SUMMARY OF LAPTOP COMPUTER SECURITY

CSG-13\S

December 2009

Canada

UNCLASSIFIED



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Laptop Security (CSG-13|S)

This page intentionally left blank.



Foreword

The *Summary of Laptop Computer Security (CSG-13\S)* is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at itsclientservices@cse-cst.gc.ca or call (613) 991-7654.

Effective Date

This publication takes effect on 12/02/2009.

Carey Frey

Director, IT Security Industry Program

© 2009 Government of Canada, Communications Security Establishment Canada

It is not permissible to make copies or extracts from this publication without the written consent of CSEC.



This page intentionally left blank.



Table of Contents

Foreword..... i

Effective Date i

Table of Contents..... iii

List of Abbreviations and Acronyms..... iv

1. Introduction 1

2. Background 1

3. Purpose..... 1

4. Scope 1

Annex A - Summary of Recommendations..... 2

Annex B -- Security Checklist 3

Annex C -- Summary of Security Issues 4

Bibliography 6



List of Abbreviations and Acronyms

AP	Access Point
BIA	Business Impact Assessment
C&A	Certification and Accreditation
CD	Compact Disc
CSEC	Communications Security Establishment Canada
DG	Director General
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
GC	Government of Canada
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	IP Security
ISP	Internet Service Provider
IT	Information Technology
ITS	IT Security
ITSA	IT Security Alert
ITSG	IT Security Guide
LCD	Liquid Crystal Display
MAC	Media Access Control
MITS	Management of Information Technology Security
NAC	Network Access Control
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
Q2	Second Quarter
RFP	Request For Proposal
SSL	Secure Sockets Layer
TRA	Threat and Risk Assessment
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2



1. Introduction

Laptop computers (laptops) are subject to all of the IT security vulnerabilities that threaten the traditional IT environment, when connected to the departmental network the laptop is protected in accordance with the department's IT security architecture. However the transportable nature of the laptop greatly increases the risk of certain vulnerabilities as compared to the traditional IT desktop environment; this document focuses on those vulnerabilities.

2. Background

Laptops represent a growing proportion of all end-user computer platforms. A key advantage of a laptop over a desktop is its portability allowing many GC users to their laptops in remote locations. Most laptops include more than 1 network connection technology; it is this inter-connectivity flexibility that renders the laptop more vulnerable to cyber threats than their desktop counterparts.

3. Purpose

This document is IT security guidance for departments to securely manage the use of laptops.

4. Scope

This document focuses on the secure use of laptops through their lifecycle.



Figure 4-1: Typical Laptops

(Image sources: first and third: Yahoo! [Reference 1][Reference 1]; second: HP Canada [Reference 2])

This security guidance is for a laptop processing and/or storing unclassified information, it does not apply to a laptop processing or storing 'Protected' or 'Classified' data. It is worth noting that while a single unit of 'data' may be 'unclassified' the *aggregate sensitivity* of a large store of that data may be greater than 'unclassified' – the aggregate sensitivity should be revealed in the TRA. If the aggregate sensitivity of a laptop's data store is greater than 'unclassified' than this security guidance does not apply to it.

This document consists of three (3) annexes that summarize the security issues with regard to Laptop Computers as discussed in the *COTS Security Guidance (CSG) Details of Laptop Computer Security (CSG-13\|G)* document. The intended audience for this document is the "Departmental Security Officer (DSO)".



Annex A - Summary of Recommendations

The table on this page summarizes the key risk mitigation strategies and policies for a typical GC environment. The ranking reflects the associated risk and priority.

<u>Risk Mitigation</u>		<u>Security Policy</u>
<p>Specification - Require host-based intrusion detection/ prevention software, firewalls, and network access control (NAC) software</p> <p>Specification - Require secure VPN connections to GC network access,</p> <p>Specification - Require disk encryption software</p> <p>Configuration - Limit privileged access</p> <p>Decommissioning - Sanitize durable memory (hard drive)</p>		<p>Specification - Require a Threat and Risk Assessment (TRA) for each unique deployment of laptop assets</p> <p>Specification - Incorporate TRA security requirements in the laptop specification/procurement process</p> <p>Configuration - Enforce 'least privilege' for the assignment of user access privileges</p> <p>Decommissioning - Develop appropriate decommissioning policy for laptop computer to ensure data confidentiality of residual data</p>
<p>Specification - Require 'anti-theft' features such as locking cables</p> <p>Configuration - Require regular updates of security-related software and data file</p> <p>Configuration - Require an active password-protected screen saver</p> <p>Configuration - Disable or remove hardware not required for work related activities (i.e. wireless network, infrared ports)</p>		<p>Specification - Develop an appropriate configuration policy for remote-use laptop computers</p> <p>Configuration - Develop policy for secure laptop configuration for remote access environments</p> <p>Configuration - If required provide 'administrator' privileges through a separate 'user-administrator' access</p> <p>Configuration - Develop an appropriate-use policy for laptop computer users that require regular software and security data files updates</p>
<p>Inventory Control - Enforce strong inventory controls</p> <p>Inventory Control - Enforce configuration management</p> <p>Decommissioning - Reconcile software and hardware with inventory control</p>		<p>Inventory Control - Develop an appropriate-use policy to prevent alterations to the deployed configuration</p> <p>Inventory Control - Develop an appropriate-use policy to restrict use to work-related activities</p> <p>Decommissioning - Develop policy to require formal decommissioning at end-of-life</p>



Annex B -- Security Checklist

This section is an IT security technology functionality requirements checklist.

Operating System Protection

- Minimal OS services configuration
- Minimal software configuration
- User Accounts configured with least-privileges
- Strong laptop-Administrator Authentication
- Strong laptop-User Authentication
- User department IT security policy training
- User appropriate-use agreement
- Anti-virus Software
- IDS Software
- IPS Software
- Encrypt wireless communications

Data Security

- Strong Passwords
- Two-Factor Authentication
- Biometric Authentication
- Data Encryption
- Encrypt stored data
- Encrypt data in transit
- User data-security awareness training

Connectivity

- Wireless connectivity only if required
- VPN connectivity for remote department access
- User network-security awareness training

Physical Security

- Secure laptop with locking cables
- User physical-security awareness training



Annex C -- Summary of Security Issues

Security Issue	Risk	Mitigation	Policy
No Threat and Risk Assessment (TRA)	The presumed threat to the laptop is underestimated resulting in an unacceptable level of risk.	Perform a TRA for the laptop and its intended operating environment.	Require a Threat and Risk Assessment (TRA) for each unique deployment of laptop assets
Incorrect Specifications	The assumed threat to the laptop is unknown resulting in an unacceptable level of risk.	Perform a TRA for the laptop and its intended operating environment.	Appropriate configuration policy for remote use laptop computers
Miss-configuration	The assumed threat to the laptop is underestimated resulting in an unacceptable level of risk.	Perform another TRA for the laptop specific to its configuration and its intended operating environment.	Appropriate configuration policy for remote use laptop computers
	The laptop cannot be used for the intended purpose. Loss of 'availability' may impact the normal business process.	Develop a Business Continuity Plan (BCP) that anticipates the loss of laptop 'availability'.	
Insufficient Inventory Control	Loss of 'availability' may impact the normal business process.	Develop stringent inventory control procedures.	Asset management policy
Loss or Theft	Laptop computers may be used in insecure environments.	IT Security Awareness Training:	The departments' appropriate Use policy for IT equipment.
	Laptop computers are high-value assets that are susceptible to crimes of opportunity.	When in use the laptop should be secured using a locking-cable. When not in use the laptop should be stored in a secure location. When being transported the laptop should never be left unattended.	Appropriate configuration policy for remote use laptop computers
	Laptop computers may contain sensitive department data the confidentiality of which may be compromised.	Protect departmental data by using data encryption along with backup and recovery procedures appropriate for a laptop.	



Laptop Security (CSG-13|S)

Security Issue	Risk	Mitigation	Policy
Unauthorized Use	Employee uses the laptop for non-work related tasks that, if publicly known, would embarrass the department.	IT Security Awareness Training: sanctions.	The departments' appropriate Use policy for IT equipment.
	Employee uses the laptop for illegal activities for which the departments may be liable.	IT Security Awareness Training: sanctions.	
	Employee allows the unauthorized use of the laptop by a third party.	IT Security Awareness Training: appropriate use.	
Insecure Use	Employee uses the laptop for work related tasks in an insecure IT environment (wireless hotspot).	IT Security Awareness Training: appropriate use. OS hardening, Security software, configuration management Secure specification and configuration	The departments' appropriate Use policy for IT equipment.
	Compromise of department data	Protect departmental data by using data encryption. Require strong user authentication, minimal ports and access protocols, firewall, IDS and IPS.	
Cyber Attack	Compromise of laptop asset.	Require strong user authentication, minimal ports and access protocols, firewall, IDS, IPS and OS hardening,	The departments' appropriate Use policy for IT equipment.
	Compromise of department data	Protect departmental data by using data encryption.	Appropriate configuration policy for remote use laptop computers



Bibliography

- [Reference 1] Yahoo! Image Search Results for laptop. In *Yahoo!* [online]. Yahoo! [cited 11 November 2008].
<http://images.search.yahoo.com/search/images?ei=UTF-8&_adv_prop=image&va=laptop&fr=slv8-&imgsz=large>.
- [Reference 2] HP Canada Consumer Laptops, Notebook Computer & Tablet PCs. In *HP Canada* [online]. Hewlett-Packard Development Company, 2008 [cited 11 November 2008].
<http://www.hp.com/canada/products/landing/notebook_tabletpc/index.html>