

UNCLASSIFIED



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

COTS SECURITY GUIDANCE (CSG)

TELEWORK SUMMARY

CSG-16\S

November 2009

2009

Canada



This page intentionally left blank.



Foreword

The *Telework Summary (CSG-16\5)*, it 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 11/27/2009.

Carey Frey
Director, IT Security Industry Program

© Government of Canada, Communications Security Establishment Canada 2009

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 Summary of Device Safeguards 5

2 Summary of Network Safeguards..... 7

3 Summary of Departmental Safeguards 8



List of Abbreviations and Acronyms

BIOS	Basic Input/Output System
CSEC	Communications Security Establishment Canada
DoS	Denial-of-Service
GC	Government of Canada
HIDS	Host Intrusion Detection System
NAC	Network Access Control
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
OS	Operating System
PKI	Public Key Infrastructure
VPN	Virtual Private Network



1 Summary of Device Safeguards

Safeguard	Benefits	Limitations
Physical protection	Thwarts opportunistic attacks. Forces attackers to use more complex and time-consuming measures.	Requires worker vigilance. Sophisticated measures can be expensive.
BIOS protection	BIOS password protects against human error. Boot password adds extra layer of security.	BIOS and boot passwords disabled by default. Can be bypassed by removing the hard drive.
Passwords	Prevents unauthorized users from accessing information on device.	Easy to forget, leading to higher help desk costs. Easy to break or circumvent.
Account privileges (Least Privilege(s))	Reduces chance that worker will change security settings. Malicious code has less ability to do damage.	Some applications may not work properly under a limited account.
Session locking	Prevents unauthorized access to unattended devices.	Like other password-based safeguards, can be circumvented.
Software updates	Ensures applications are not vulnerable to known exploits.	Can use up bandwidth and system resources. Can occasionally reduce performance of application or device.
File encryption	Relatively simple and fast.	Does not encrypt paging or temporary files. Relies on worker remembering to use it.
Folder encryption	Less reliance on worker. Can encrypt some temporary files.	Does not encrypt files in non-protected folders. Does not encrypt paging files.
Whole disk encryption	Encrypts all files, including paging and temporary files. Convenient; no worker intervention.	Slower than other types of encryption. It can be difficult to recover from disk failure.
Anti-virus and anti-spyware software	Best defence against malicious code, which is the most common threat.	Needs to be updated regularly.



Summary on Telework (CSG-161S)

Safeguard	Benefits	Limitations
HIDS	May detect attacks that bypassed preventive safeguards.	May generate false alarms. Uses some system resources while running.
Application security	Contributes to overall security.	Difficult to maintain secure configuration after device issuance. Worker has to bring device into office for application maintenance.
Content filtering	Blocks many types of malicious code and inappropriate content.	May require ongoing maintenance to ensure access to required sites is allowed.
Security maintenance and monitoring	Ensures device remains in secure state. Increases worker awareness of security.	May be beyond capabilities of some workers.
Backups	Prevents loss of valuable information if device is compromised, lost or damaged.	More difficult in situations where remote mobile device is not connected to departmental network; removable media and worker participation are required in such cases.



2 Summary of Network Safeguards

Safeguard	Benefits	Limitations
Strong identification and authentication	Better than simple passwords. Helps against replay attacks.	Some methods require synchronization between endpoints. If using PKI for authentication the PKI infrastructure must set up and maintained.
VPN encryption	Provides confidentiality, integrity, and strong authentication.	Some implementations require VPN client on remote mobile devices, which uses processing cycles. May be incompatible with some firewalls.
Enterprise and personal firewalls	Protect endpoints against network-based attacks from the Internet.	Must be properly configured. May be incompatible with some VPNs.
NIDS	Can detect attacks that get past firewalls. Cannot be detected by attackers. Will not disrupt traffic.	May generate false alarms. Requires constant monitoring. Cannot stop attacks in progress.
NIPS	Can respond to attacks (unlike NIDS). Can protect against DoS attacks.	May respond to false alarms, disrupting authorized traffic.
NAC	Ensures remote mobile devices are up to date in terms of patches, signatures, etc.	Immature products may not work as advertised.
Home network security	Significantly reduces risks to remote mobile devices from Internet attacks.	Some expenses (such as broadband router) may have to be borne by teleworker. Configuring home network security may be beyond capabilities of some teleworkers.
Call-back modems	Provides a form of mutual authentication.	May be difficult to source and purchase. Direct-dial connections are slow and inconvenient.



3 Summary of Departmental Safeguards

Safeguard	Benefits	Limitations
OS hardening	Reduces risks of OS vulnerabilities being exploited.	Labour-intensive. Requires constant monitoring.
E-mail security	Enhances confidentiality and integrity of messages. Also offers non-repudiation and authentication.	Not all solutions are interoperable. PKI required.
Operational security	Helps ensure that technical security controls work correctly. Supports ongoing security through incident response.	Requires skilled personnel, which can be expensive.