Pages 1 to / à 10

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 16(2)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information
Loi sur l'accès à l'information

OPS-5-1

Operational Use of the Internet

Table of Contents

1. Overview

1.1 Objective

These procedures provide guidance on accessing the Internet for operational reasons. Specifically, these procedures will:

- Identify the types of Internet activities that are conducted for operational reasons;
- Identify the risks associated to these activities;
- Define what systems must be used for these activities; and
- Describe best practices.

Note: internet systems used for operational reasons are under review and are not discussed in these procedures; but will be included in future revisions.

1.2 Context

The Internet is a source of UNCLASSIFIED information, which staff can incorporate into certain product, and/or use as lead information in further research and analysis.

These procedures are required to help ensure that:

-
- and
-

1.3 Application

These procedures apply to CSE and staff who use the Internet to conduct research related to their job, as well as other parties conducting operations under CSE authorities.

1.4 CSE Internet Policy

These procedures complement the *CSE Internet Policy* (previously known as CPP-1085).

1.5 Previous Procedures

These procedures supercede *Approved Systems for Internet Activities*, 7 May 2002.

1.6 Accountability

The following table outlines the responsibilities of the various players vis-à-vis these procedures.

Who	Responsibilities
DC SIGINT DC ITS DC CS	• Approving these procedures • Applying these procedures
DG Policy and Communications CIO/CTO	• Recommending these procedures for approval
Manager, Operational Policy	• Revising these procedures • Approving changes to Annexes • Seeking legal advice when required
Manager, Information Protection Centre (IPC)	Updating Annexes
CSE and Staff	Reading, understanding and complying with these procedures and any amendments to these procedures

1.7 Reference

CSE Internet Policy, dated 15 December 2004

1.8 Enquiries

Questions related to these procedures should be directed to operational managers who in turn will consult the CSE Operational Policy Section if necessary.

1.9 Amendments

Situations may arise where amendments to these procedures may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted on the Operational Policy website at

2. Internet Activities and Their Associated Risks

2.1 Types of Internet Activities

The different types of Internet Activities carried out by CSE and staff for operational reasons include:

- Non-sensitive web surfing;
- E-mail;
- Web research using Subscription services;
-
-
-
- and email.

2.2 Non-Sensitive Web Surfing

Non-sensitive web surfing refers to visiting Web sites that, if revealed, would not cause embarrassment to CSE, This type of activity is carried out via See the *CSE Internet Policy* for more information on the use of the Internet for non-sensitive web surfing.

Example of Non-sensitive web surfing:

- Staff visit on-line news services.

Note: Staff must not use

2.3 E-mail

Staff must be careful when sending/receiving e-mails via because their names and their link to CSE are attached as header information on these emails.

2.4 Web Research Using Subscription Services

Staff may access various commercial databases available through CSE's Library Information Services. These commercial databases provide access to thousands of journals and reports.

Note: If staff incorporate any Open Source information from these commercial databases into a report, they must also quote or cite the Open Source somewhere in the report. CSE's Library Information Services can provide related guidance.

Staff should consult with their supervisors if they have any questions about which searches may be conducted.

This type of Internet activity refers to

(see Annex 2 for matrix of approved systems vs Internet activities).

This type of Internet activity refers to

(see Annex 2 for matrix of approved systems vs Internet activities).

Related examples:

Note: Section 3 provides tips on how to further when conducting this type of activity.

This type of activity refers to

(See Annex 2 for matrix of approved systems vs Internet activities.)

Staff must use a system that

(see Annex 2 for matrix of approved systems vs Internet activities).

Note 1: In certain situations, a Level IV operational manager may authorize an analyst to

- an operational requirement exists;
- and
- The has been consulted.

3. Best Practices

3.1 Introduction

The use of a system with lowers the risk that a person's
However, staff must also adopt other practices so as to further reduce the probability that
These practices may also help reduce the risk of

Caution: must not be used for searches. Staff should consult with their supervisors if they have any questions about what activities may be conducted on or on systems with

The Internet activities described in Section 2 present various levels of security risk to CSE and its staff. These risks can be mitigated by using the appropriate system that has been approved by
The systems currently approved are described in Annex 1. The table in Annex 2 identifies what systems to use for the different Internet activities described in Section 2.

3.4 Avoiding "Honeypots"

to an unknown site that is referenced at a Web site intended for a limited audience. This site may be a "honeypot" which has been intentionally created to identify unwelcome visitors.

Tip:
To avoid accessing potential honeypots,

4. Definitions

4.4 Attack	An attack is an attempt to gain unauthorized access to an Internet user's services, resources, or information, or the attempt to compromise an Internet user's integrity, availability, or confidentiality.
4.5 Compromise	A compromise is an unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

s CSE's unclassified network that provides access to the Internet. It is secure up to the PROTECTED B level.

Annex 1: Current Systems Approved for Internet Activities

A1.1
Introduction

(See Annex 2 for the matrix of Approved systems vs Internet activity).

is CSE's unclassified network that provides access to the Internet. It is secure up to the evel.

When surfing the Web via However, if staff use to send emails, or to complete on-line forms,

Pages 22 to / à 23

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 16(2)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information
Loi sur l'accès à l'information

s.15(1)

s.16(2)(c)

s.21(1)(a)

Annex 2 : Matrix of Approved Systems vs Internet Activity

If you need to Conduct …	Then use…
Non-sensitive web surfing	
E-mail	
Web research using subscription services	

Approval Authorities:

OPS-5-1 Promulgation

I hereby approve OPS-5-1, *Operational Use of the Internet.* These procedures are effective immediately.

_____ _____

Robert Brûlé
Deputy Chief SIGINT

Date

_____ _____

Michael Devaney
Deputy Chief ITS

Date

_____ _____

Barb Gibbons
Deputy Chief Corporate Services

Date

Reviewed and Recommended for Approval:

_____ _____

John Ossowski
Director General Policy and Communications

Date

_____ _____

Peter Laneville
Chief Information Officer/Chief Technology Officer

Date