Industry Canada Industrie Canada

Client Services Branch
Chief Information Office Sector
Information Technology Security

IT Security

IT: Security is the key

http://icweb.ic.gc.ca/946-5555
(613) 946-5555
E-mail: CIOCENTRE@ic.gc.ca

Canada

Who Are We?

Information Technology (IT) Security experts help ensure you are working in a secure technical environment at Industry Canada (IC).

The IT Security team offers practical advice and guidance on how to keep your computer networks secure and virus-free.

Our Mission

IT Security's mission is to:

- provide reasonable, effective and timely IT and communications security measures;
- anticipate the future needs of IC employees and provide a secure framework on which to build the infrastructure;
- anticipate future threats and risks, and take appropriate steps to eliminate or mitigate their effects; and
- respond professionally and in a timely fashion to incidents that could compromise the safety and security of all assets in our care (i.e. personnel, data or physical objects).

Our Focus

IC's network is an essential work tool. IT security protection procedures have been put in place to ensure it works smoothly without interruption.

Our objectives are to:

- continually improve best practices for IT security;
- inform employees of virus protection procedures and virus alerts when necessary;
- advise employees on how to secure classified electronic documents;
- provide assistance to business units in planning Threat and Risk Assessments and Statements of Sensitivity;
- promote secure communications; and
- provide IT security awareness briefings on various topics for new employees, individual business units, and so on.

Best Practices for IT Security

Passwords

Your password secures your workstation. Follow these important tips to keep your computer secure:

Do

- lock your computer with a password when leaving your desk; and
- choose a strong password (seven characters, alphanumeric, no dictionary words).

Don't

- leave your password written down near your computer;
- simply add a number to the end of your password when you are prompted to change it; and
- give out your password.

Unsolicited Spam E-mail

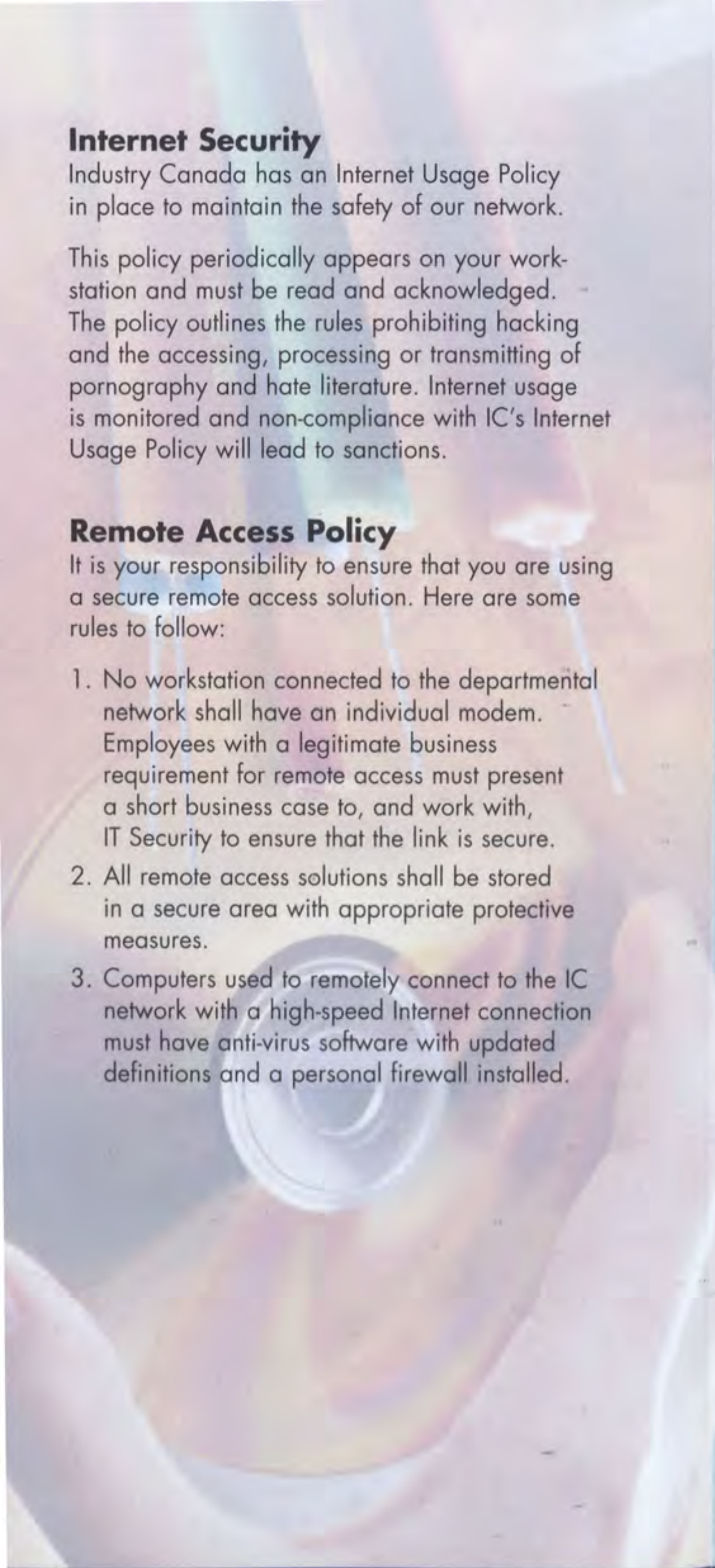
Unsolicited spam e-mail enters the IC network daily, advertising a variety of products or services, including pornography.

You may be tempted to unsubscribe from receiving further spam e-mail by replying to such messages. However, this may result in an increase in the amount of spam e-mail you receive.

Instead, IC employees are encouraged to:

- delete spam e-mails;
- minimize the likelihood of receiving unsolicited spam e-mail; and
- complain to the spam sender's Internet Service Provider (ISP).

Note: See the MS Outlook Coaching Tips "How do I get rid of spam e-mails addressed to me" and "How do I submit a complaint with the offender's Internet Service Provider" on the CIO IT Call Centre Web site for more information.



Internet Security

Industry Canada has an Internet Usage Policy in place to maintain the safety of our network.

This policy periodically appears on your workstation and must be read and acknowledged. The policy outlines the rules prohibiting hacking and the accessing, processing or transmitting of pornography and hate literature. Internet usage is monitored and non-compliance with IC's Internet Usage Policy will lead to sanctions.

Remote Access Policy

It is your responsibility to ensure that you are using a secure remote access solution. Here are some rules to follow:

1. No workstation connected to the departmental network shall have an individual modem. Employees with a legitimate business requirement for remote access must present a short business case to, and work with, IT Security to ensure that the link is secure.
2. All remote access solutions shall be stored in a secure area with appropriate protective measures.
3. Computers used to remotely connect to the IC network with a high-speed Internet connection must have anti-virus software with updated definitions and a personal firewall installed.

Laptops

Laptops are easy targets for thieves because of their size, value and accessibility to sensitive information. Here are some guidelines to keep your laptop secure:

1. Tie it down using a cable locking system.
2. Install a tracking device.
3. Have a strong password.
4. Backup the data on the C drive regularly.
5. Use encryption to protect data.
6. Lock it up in a cabinet or safe when not in use.
7. Always carry-on your laptop when boarding a plane and ensure your battery is charged.

Virus Attacks

All virus incidents are considered urgent. If you have a virus:

- immediately unplug your computer from the network (cable resembling a telephone cord); and
- contact the CIO IT Call Centre for further instructions.

IT Alerts

Should a virus threaten the IC network, a virus alert will be posted on ICWeb and on the CIO IT Call Centre Web site.

There are three virus alert levels — green, yellow and red — which outline the computer virus protection protocol.

A red virus alert means that the network is under virus attack and all employees are instructed to shut down their computers immediately.

Public Key Infrastructure (PKI)

All IC employees can have a PKI key, which is needed to secure e-mail messages or to protect data.

Threat and Risk Assessments

IT Security must be contacted before implementing any new or updated on-line applications in your business unit. IT Security provides assistance in planning Threat and Risk Assessments and Statements of Sensitivity.

Communications Security

Communications security (COMSEC) is administered by IT Security. Requirements for STU–III telephones, virtual private network accounts and other secure communications methodologies should be discussed with the IT Security team.

IT Security Awareness

Awareness briefings on general IT security and various specialized topics are provided by IT Security.

Awareness briefings for new employees and customized presentations at your business unit staff meetings or focus days are available upon request.

How to Contact Us

We welcome your comments, concerns, questions or suggestions. To learn more about the topics in this brochure, contact us at the following:

Address: C.D. Howe Building
235 Queen Street
Ottawa ON K1A 0H5

Fax: (613) 946-3367

Web site: http://icweb.ic.gc.ca/946-5555

For information or urgent matters:

Tel.: (613) 946-5555
E-mail: CIOCENTRE@ic.gc.ca

For security incidents or confidential matters:

Tel.: (613) 998-3209 or (613) 957-8625
E-mail: ITSECURITY@ic.gc.ca

IT security is everyone's responsibility.

53662B
March 2002

10% recycled material