2020-04-30

Five Key Security Responsibilities You Need to Know

1) PROTECTING SENSITIVE INFORMATION

- As you carry out your duties, including working from home, you may be privy to sensitive information. Sensitive information is identified and categorized as Protected A (e.g. home address), Protected B (e.g. medical records), Confidential (e.g. financial or technical records) or Secret (e.g. Treasury Board Submissions). Note: “Secret” level security clearance is required to access Confidential and Secret information.
- You are responsible for ensuring that sensitive information under your care, even at home, is properly identified, transported, stored and disposed - http://intranet2/media/2612702/soi_-_bilingual_.pdf (available only when logged into the Parks Canada Network)
- Discuss and handle sensitive information with discretion. Share sensitive information only with authorized colleagues who have the need to know and who possess the appropriate security level.

2) PROTECTING ASSETS

- Parks Canada assets must be kept secure from unauthorized access, theft or vandalism, even at home.
- Do not share keys, combinations, access codes, PINs or your ID card with unauthorized individuals.
- Be vigilant and take appropriate action if you see unauthorized individuals in areas restricted to Parks Canada team members and sites closed to the public.
- Anyone who has not been given clearance by the Departmental Security Office and is going beyond the reception area of an office building should sign in by giving their name, business, and contact within the building.
- Parks Canada property and assets can only be used in the conduct of your official duties, not for personal gain or use.
- You can request specific security advice such as the procurement of cameras for a particular site through the Security Service Desk offered by the Departmental Security Office.

3) ACCEPTABLE USE OF ELECTRONIC NETWORKS AND DEVICES

- The Government of Canada's Guideline on Acceptable Network and Device Use outlines that electronic networks and devices may only be used:
    - to perform activities that are part of your official duties.;
    - for career development and other professional activities.
    - for limited personal use that is conducted on personal time; that is not for financial gain; that does not incur any additional costs to Parks Canada; and that does not interfere with the conduct of business.

Click here and then on "IT Security and Working from Home" to learn more: https://parkscanada.atlassian.net/servicedesk/customer/portal/2/article/196610?src=1656740508

- Visit GetCyberSafe.gc.ca and Cyber.gc.ca for more on how to stay cyber secure

4) REPORTING SECURITY INCIDENTS

- As a Parks Canada employee, contractor or volunteer, you are the "eyes and ears" to help keep our workplace secure.
- Security incidents (e.g. theft, break-ins, loss of keys, vandalism, unauthorized disclosure of information, unauthorized access) may occur in your workplace, even at home.
- You are responsible for reporting any security incident involving Parks Canada information or assets to your supervisor, manager or the Departmental Security Office.

5) REPORTING CHANGES IN PERSONAL CIRCUMSTANCES

- Even during these challenging times, you are responsible for reporting any information related to a change in personal circumstances that may affect your security status or clearance (e.g. criminal charge or conviction, suspect in a criminal investigation, judicial prohibitions) to your supervisor, manager or the Departmental Security Office.

CONTACT

pc.securite-security.pc@canada.ca

Security Service Desk (available only when logged into the Parks Canada Network):
http://jira/servicedesk/customer/portal/14