IT SECURITY POLICY SUMMARY

Overview of the Information Security Policy

The Air Canada Information Security Policy is a set of policies and requirements that define the fundamental principles for the protection of information assets and the proper controls needed to ensure compliance with internal and external regulations.

The Information Security Policy (ISP) applies to all Air Canada employees (including retirees) and agents (which means any person performing tasks on behalf of or for the benefit of Air Canada but who is not an employee).

The ISP also applies to all corporate information and personal information (whether it pertains to employees, agents, customers, suppliers, or other members of the public) as well as to all information management systems (including all application systems, websites, processes, facilities, equipment and documentation) that belong to, are used by or are in the custody of Air Canada, regardless of their form or location.

Purpose of the Information Security Policy

The main purpose of the Information Security Policy is to prevent or minimize the likelihood and impact of information security breaches. It is also to enhance the protections accorded to Air Canada information assets. Information security breaches that could impact Air Canada operations include:

- Unauthorized access to information,
- Unauthorized or unintentional disclosure or leakage of information,
- Data tampering or vandalism, and
- Destruction or interference with computing systems leading to system outages or failures

Personnel Responsibilities

Things to Do:

- Become familiar with and abide by the Air Canada Information Security Policy
- Comply with applicable Air Canada operating policies, legislation, vendor contracts, non-disclosure agreements, copyrights and patents.
- Protect information assets against accidental or unauthorized modification, disclosure, or destruction while in your possession.
- Obtain individual authorization through official channels to obtain access to systems and to use, disclose, or modify protected information.

Things to Avoid:

- Sharing of user IDs, access codes or passwords.
- Subversion, bypass or corruption of security measures such as anti-virus or firewalls on Air Canada computers.

Things to pay attention to:

- Information regarding policies and procedures for information protection.

Things to report:

- Confirmed or suspected loss or theft of a computer, electronic device or communication system access token (e.g. Blackberry®, cell phone) to Corporate security in a timely manner
- Notifying the System Authorizer when access to the system is no longer required.

Management Responsibilities

Things to do:

- Understand policies and practices regarding information security.
- Ensure that each staff member is fully aware of this policy and of any legal restrictions on accessing, handling, collecting and disclosing information available to them.
- Ensure that you authorize all information system access for users reporting to you.
- Promptly report to the appropriate Authorizers changes in status (e.g. reassignment, termination etc.) of users reporting to you which may affect information access rights.

Things to reinforce with personnel:

- The importance of understanding policies, adhering to standards and following approved processes.

Things to report:

- Promptly report any suspected security breach to corporate security in a timely manner.

IT Personnel Responsibilities

Things to do:

- Master the Security Standards described in the Information Security Policy and manage the IT resources for which you are responsible in compliance with these standards.
- Ensure that the passwords for the systems and applications you manage meet the requirements of the Information Access Control Policy.
- Configure all Air Canada-owned and managed IT devices/systems to enforce the password policy to the degree technically feasible, in compliance with the Information Access Control Policy.
- Address system and application vulnerabilities within the timeframes specified in the IT Operations Security Policy.

Things to avoid:

- Not patching the IT systems for which you are responsible for.
- Taking action that might inhibit investigation of an incident or make unavailable information that might assist the investigation.

Things to report:

- Report immediately any suspected compromise of the security of sensitive data or mission critical systems (e.g. ERP, Payroll, corporate email, etc.).

References (Policy numbering)

Documentation	Description
Information Security Policy	
01	Information Security Governance Policy
02	Information Asset Management Policy
03	Personnel Security Policy
04	Physical Security Policy
05	Information Access Control Policy
06	Logging Policy
07	Cryptography Policy
08	Application Development Policy
09	Change Management Policy
10	Backup Media Handling Policy
11	IT Operations Security Policy
12	Security Incident Response Policy
13	System Security Policy
14	Network Security Policy
15	Service Provider Policy
16	IT Acceptable Use Policy
17	Policy Enforcement Policy

Key Contacts

Contact	Link
Office of the Chief Information Officer	lise.fournel@aircanada.ca
IT Security and compliance Manager	Paul.Assaad@aircanada.ca