Acceptable Use Agreement for Government-Provided Computer Technology

Introduction:

This agreement is in place to protect employees, the employer and the information in the Governments custody or under the control of a public body. It applies to all employees, independent contractors, temporary workers and all other individuals using Government owned electronic information resources.

The confidentiality, integrity and availability of computer technology used inside or outside the work place, that contains client and personal information, must be preserved at all times. Access to this Government-provided technology is granted under the following conditions:

1. Government-provided computer technology is to be used to support authorized programs and services.
2. Users must use only system information technology they are authorized to use and use them only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.
3. Changing the Government –provided computer system configuration is not permitted unless approved by End User Support.
4. Personal use of Government-provided computer technology is to be of an appropriate nature that will not incur additional cost or increased risk to the Government. Such technology is not to be used for any personal activity that may cause embarrassment to you or the Government and must not be used to access or promote inappropriate sites, including but not limited to pornography, racism, hatred, gambling, obscenity or any illegal activities.
5. You are responsible and accountable for the use of your user ID, passwords and other access control items in your possession for computer technology. They are not to be shared.
6. The bandwidth available to Government is limited. Therefore the use of streaming audio and video (e.g. Online radio, YouTube, etc.) should be limited to a work related need.
7. Removal of, or alterations to, Government-provided computer hardware or components must be approved by End User Support.
8. Prior to downloading or installing software on Government-provided hardware confirmation of acceptability must be obtained from your Departmental Information Technology Architect (ITA).
9. You must not violate the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Technical ability to access other's accounts does not, by itself, imply authorization to do so.
10. You should not leave your computer unattended while logged on to the network. A password protected screen saver is required to reactivate a session after 5 minutes of inactivity.
11. Work related electronic data must be stored on the Government-provided file server where possible. If work related electronic data is not stored on the file server it is your responsibility to prepare and maintain backup copies in accordance with Government Policies, the *Archives and Records Act* and the *Freedom of Information and Protection of Privacy Act.*
12. Wilful or intentional violations of this agreement will be considered to be misconduct and violators of this agreement may be denied access to the Government-provided computer technology and may be subject to other penalties and disciplinary action in accordance with the *Civil Service Act* and Regulations. Violation of this Agreement may result in discipline that may include but not be limited to termination or employment and/or other legal action.

I have read and understand "The Acceptable Use Agreement for Government –Provided Computer Technology" and recognize that technical monitoring takes place to protect the system and ensure users are complying with this policy. I agree to access and use the Government-provided computer technology only in accordance with the terms and conditions set out in this Agreement.

Date: _____ Name of User: _____
(Please Print)

Witness: _____ User Signature: _____

Definitions:

Acceptable Use Policy (AUP) is a written agreement all users of the Government-provided computer technology adhere to for the common good. An AUP defines the intended uses of the network including unacceptable uses and the consequences for non-compliance.

Computer Hardware refers to workstations, stand alone computers, network computers, laptops, notebooks, servers, PDAs, Blackberries and any other peripherals.

Computer Software refers to written programs, procedures or rules and associated documentation pertaining to the operation of a computer system, which includes packaged software, downloadable executables, screen savers, macro, freeware and shareware.

Computer Technology, for the purpose of this agreement, is Computer Systems and all electronic data.

Electronic Data is data that is stored and readable in electronic form without regard to the hardware or software used to produce the data, excluding computer software.

Office of Information is the designated authority responsible for maintaining and monitoring compliance with Government Security Policies and Directives.

SecurID: is a mechanism developed for performing two-factor authentication for a user to a network resource.

Token: are used to prove one's identity electronically. The token is used in addition to or in place of a password to prove that the employee is who they claim to be. The token acts like an electronic key to access something.

Virtual Private Network (VPN): is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling user's access to a central organizational network.

Disciplinary Action:

Please take the time to peruse the following two links. It will be useful in explaining where the discipline consequence arise from any violation.

1. Treasury Board – Section 16.02 – Security Policies: http://iis.peigov/dept/tboard/manual/pdf/sec1602.pdf

2. *Civil Service Act* and Regulations :
   Section 31 – 33 of the CSA Regulation: http://www.gov.pe.ca/law/regulations/pdf/C&08G.pdf