# VPN Request Instructions

1. All sections are to be completed unless otherwise noted. Only forms which are properly completed will be accepted. Incomplete forms will be returned.

2. This form must be submitted electronically via e-mail to: servicecentre@gov.pe.ca, in a PDF or scanned to JPG format but we do not accept electronic signatures. Please allow 5-10 business days for delivery after this approval has been received

3. Service Centre will validate that the individual requesting access is an employee of the Government of Prince Edward Island; or that the request from a non- government employee is being made on behalf of a sponsoring department or agency. The requirements will be validated and requests may be returned for clarification.

4. Any management authority of the government may immediately request the suspension of remote access service for individuals found to have violated the Terms and Conditions for remote access. This can be accomplished by contacting the Service Centre at 620-3600. The Service Centre will then initiate a process to verify this request.

5. Temporary accounts will be terminated on the listed end date. If an extension is required, submit your request to the servicecentre@gov.pe.ca at least 2 weeks prior to the end date.

## Contact Information:

IT Shared Services
Phone (902) 620-3600
Fax (902) 368-4716
email: servicecentre@gov.pe.ca

November, 2017

# VPN Request Form - External Users

## VPN Access Request

| Government Department |
| --- |
| |

## User Information

| First Name | Last Name | Initial | Email |
| --- | --- | --- | --- |
| | | | |

| Organization | Position | Office Phone |
| --- | --- | --- |
| | | |

## Government Departmental Signing Authority

| Name | Phone | Email |
| --- | --- | --- |
| | | |

| If this is for a temporary account please enter complete end date (m/d/y) | |
| --- | --- |

| Rationale: Please provide an explanation as to why a VPN account is required to fulfill your employment duties with the Province. |
| --- |
| |

| Specific Application or Service (i.e. ISM, FIS, RIS/PACS, CIS) Please list below: |
| --- |
| |

# VPN Access Authorization

By Activating this Remote Access Service, You agree that you have read and understand the Terms & Conditions under which access to the Government of Prince Edward Island Computer Network is granted.

## Terms and Conditions

1. To gain access to the Province of Prince Edward Island's Government Network, you must enter a valid username and password.
2. Employees shall be held accountable for all activities while using the VPN account. Sharing of username and password is forbidden.
3. Access shall be limited to authorized individuals with a demonstrated business purpose only.
4. All information accessed remotely shall be held with the same confidentiality levels as the employee's on- site connection at the Government of Prince Edward Island.
5. Login ID's must be kept confidential. Report immediately any suspected compromise of this confidentiality to the Service Desk at 620-3600.
6. Non-government assets that are used to connect to the government network will be required to pass an automated security posture check to ensure that these systems meet the base security requirements for access (i.e. anti-virus active and up-to-date, no known Trojans or other malware). Systems that do not meet the requirements will not be permitted access until identified deficiencies are corrected. Please contact the Service Desk if your system fails the security check.
7. Remote access sessions may be monitored and periodic audits may be carried out.
8. All VPN users are required to adhere to all Government of Prince Edward Island information technology policies, guidelines, directives and procedures related to network and application data access.
9. 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 is not limited to termination of employment and/or other legal action.

**User:** I have read and understand and agree to the Terms for Remote VPN Access provided as part of this form.

| User Signature | Date |
|---|---|
| | |

**Deputy Head / Manager:** I agree to the Terms for Remote Access and have the supervisory authority to agree and commit to them.

| Government Departmental Signature | Date |
|---|---|
| | |

***Please note this form must be accompanied by a signed Acceptable Use Agreement***

# Acceptable Use Agreement

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 Consultant (ITC).

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. Willful 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.

13. I understand and agree that when my employment with Government ceases, for whatever reason, my authorization to use the Government-provided computer technology and system also ceases.

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. **(Please type or print)**

| Name of User | User Signature | Date |
|---|---|---|
| | | |
| Name of Witness | Witness Signature | Date |
| | | |

# 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 executable, 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.

Electronic 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.

Remote Desktop Protocol (RD) is a proprietary protocol which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client's software for this purpose, while the other computer must run RDP server software.

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.