DGSI Information Technology

VPN Access Request Form

Impact Statement and Instructions for Use

Virtual Private Network

Virtual Private Networks (VPN) provide easy access from the Internet to a private network and its internal resources. VPN security is only as strong as the methods used to authenticate the users (and the devices) at the remote end of the VPN connection. The Director of IT **must** sign this form for the request to be granted.

Unguarded computing habits can lead to malware infections potentially resulting in a multitude of detrimental effects, from the widespread exposure of sensitive information stored on the device, to compromising the performance and security of the entire DGSI network environment.

Following the precautionary policies, guidelines, recommendations and instructions outlined below will help minimize the security risks of using a VPN, and ensure that you conform with DGSI's information security policies.

DGSI Information Security website: http://security.dgsi.ca

1. All VPN requests should start with a request submitted to the DGSI Help Desk. Please complete the form below. The completed and signed form is then returned to the IT Help Desk, (helpdesk@dgsi.ca) which scans it, creates a ticket and assigns the ticket to complete.

If the form is filled out correctly and signed by the correct manager we will continue to the next step. If not, the form must be amended and submitted again.

2. When this is completed, for DGSI PC's only - we check the user's computer for virus and malware, after which we ensure that the computer is installed with the latest security updates for their operating system.

For home systems it us the responsibility of the employee to ensure their PC is secured against any risk. For guidelines regarding recommended steps to do so, please visit http://security.dgsi.ca/en/DGSI IT End User PC Best Practices

It is critical that if connecting from your home computer, it has the most recent security patches for your operating systems. Visit http://update.microsoft.com for windows OS or http://www.apple.com/support/downloads/ for MAC OS. Anti--virus software MUST be installed with the latest definition file and updates (ie. McAfee virus scan, Norton anti--virus, AVG, Avast etc).

3. At this point we will configure your account to allow VPN access and will notify you when complete. Follow the instructions at http://security.dgsi.ca/en/DGSI_VPN_Client_Install.pdf to perform the component installation to connect the DGSI network.

JUSTIFICATION FOR VPN ACCESS:			
☐ System Administration	☐ Remote Control of Work PC	☐ File Access	☐ Other (Specify Below)

SYSTEM(S) YOU NEED TO ACCESS FOR REMOTE CONTROL: (Ask IT for help if this information is unknown)	
IP Address	**Computer Name**

WHAT APPLICATIONS AND RESOURCES WILL YOU ACCESS: (i.e. STAFFNET, GP, Avanti, etc...)

EMPLOYEE INFORMATION:	
Last Name:	First Name:
Phone:	Email:
Branch or Department:	
Duration of Access (end date): / /	

INFORMATION SECURITY STATEMENT:

I have read, and agree to abide by the DGSI Acceptable Use of Computer Resources Policy found at http://security.dgsi.ca/en/DGSI Acceptable Use of Computer Resources

Employee Signature: Date:

For Home Use:

I hereby certify that the computer used to connect to DGSI via VPN has the most recent operating system updates, has been checked for malware and has a regularly updated anti-malware package installed and I will continue to ensure these are maintained

Employee Signature: Date:

APPROVALS:	
Supervisor's Name:	
Supervisor's Signature:	Date:
CEO, CFO or Director of IT:	
CEO, CFO or Director of IT Signature:	Date: