
# PGF CAPITAL BERHAD

# IT POLICY

(Version 4: approved on 20 January 2025)

# 1. Acceptable use of Information System

1.1 **PURPOSE**

The purpose of this policy is to outline the acceptable use of computer equipment at PGF. These rules are in place to protect the authorized user and PGF. Inappropriate use exposes PGF to risks including virus attacks, compromise of network systems and services, and legal issues.

1.2 **SCOPE**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct PGF business or interacts with internal networks and business systems, whether owned or leased by PGF, the employee, or a third party.

All employees, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with PGF policies and standards, local laws, and regulations.

1.3 **DEFINITION**

1.3.1 **Information Systems -** All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of administrative, instructional, research, or service activities.

Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

1.3.2 **Authorized User -** An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

1.3.3 **Extranet -** An intranet that is partially accessible to authorized persons outside of a company or organization.

1.4 **POLICY DETAIL**

1.4.1 **Ownership of Electronic Files -** All electronic files created, sent, received, or stored on PGF owned, leased, or administered equipment or otherwise under the custody and control of PGF are the property of PGF.

**Privacy -** Electronic files created, sent, received, or stored on PGF owned, leased, or administered equipment, or otherwise under the custody and control of PGF are not private and may be accessed by PGF MIS Department at any time without knowledge of the user, sender, recipient, or owner.

1.4.2 Electronic file content may also be accessed by appropriate personnel in accordance with directives from Human Resources or the CEO.

1.4.3 **General Use and Ownership -** Access requests must be authorized and submitted from departmental supervisors for employees to gain access to

computer systems. Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the corporate systems immediately become the property of PGF. Because of the need to protect PGF's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to PGF.

For security and network maintenance purposes, authorized individuals within the PGF MIS Department may monitor equipment, systems, and network traffic at any time.

PGF's MIS Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

PGF's MIS Department reserves the right to remove any non-business-related software or files from any system.

Examples of non-business-related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

1.4.4 **Security and Proprietary Information -** All mobile and computing devices that connect to the internal network must comply with this policy.

System level and user level passwords must comply with the Password Policy. Authorized users must not share their PGF login ID(s), account(s), passwords, Personal Identification Numbers (PIN), or similar information or devices used for identification and authentication purposes.

Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorized users may access, use, or share PGF proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.

All users must lockdown their PCs, laptops, and workstations by locking (ctrl-alt-delete > Lock) when the host will be unattended for any amount of time.

PGF proprietary information stored on electronic and computing devices, whether owned or leased by PGF, the employee, or a third party, remains the sole property of PGF. All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of PGF proprietary information to their immediate supervisor and/or the MIS Department.

All users must report any weaknesses in PGF computer security and any

incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the MIS Department.

Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

1.4.5 **Unacceptable Use -** Users must not intentionally access, create, store, or transmit material which PGF may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, contractor, consultant, or temporary employee of PGF authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing PGF-owned resources.

1.4.6 **System and Network Activities -** The following activities are prohibited by users, with no exceptions:

(i) Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by PGF.

(ii) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PGF or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to PGF MIS Department.

(iii) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(iv) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

(v) Using a PGF computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

(vi) Attempting to access any data, electronic content, or programs contained on PGF systems for which they do not have authorization, explicit consent, or implicit need for their job duties.

(vii) Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of PGF MIS Department.

(viii) Installing or using non-standard shareware or freeware software without PGF MIS Department approval.

(ix) Installing, disconnecting, or moving any PGF owned computer equipment and peripheral devices without prior consent of PGF's MIS Department.

(x) Purchasing software or hardware, for PGF use, without prior PGF MIS Department compatibility review.

(xi) Purposely engaging in activity that may;
- Degrade the performance of information systems;
- Deprive an authorized PGF user access to a PGF resource;
- Obtain extra resources beyond those allocated; or
- Circumvent PGF computer security measures.

(xii) Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, PGF users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on PGF information systems. The PGF MIS Department is the only department authorized to perform these actions.

(xiii) Circumventing user authentication or security of any host, network, or account.

(xiv) Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).

(xv) Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Access to the Internet at home, from a PGF-owned computer, must adhere to all the same policies that apply to use from within PGF facilities. Authorized users must not allow family members or other non-authorized users to access PGF computer systems.

PGF information systems must not be used for personal benefit.

1.4.7 **Incidental Use -** As a convenience to the PGF user community, incidental use of information systems is permitted. The following restrictions apply:

(i) Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.

(ii) Incidental personal use of electronic mail, internet access, printers, copiers, and so on, is restricted to PGF approved users; it does not extend to family members or other acquaintances.

(iii) Incidental use must not result in direct costs to PGF without prior approval

of management.

(iv) Incidental use must not interfere with the normal performance of an employee's work duties.

(v) No files or documents may be sent or received that may cause legal action against, or embarrassment to, PGF.

(vi) Storage of personal email messages, voice messages, files, and documents within PGF's information systems must be nominal.

(vii) All messages, files, and documents - including personal messages, files, and documents - located on PGF information systems are owned by PGF, may be subject to open records requests, and may be accessed in accordance with this policy.

## 2. Account Management

2.1 **PURPOSE**

The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at PGF.

2.2 **SCOPE**

This policy applies to the employees, Directors, contractors, consultants, temporaries, and other workers at PGF, including all personnel affiliated with third parties with authorized access to any PGF information system.

2.3 **DEFINITION**

**Account -** Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

**System Administrator -** The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

2.4 **POLICY DETAIL**

2.4.1 **Account**

(i) All accounts created must have an associated written request and signed management approval that is appropriate for the PGF or service.

(ii) All accounts must be uniquely identifiable using the assigned username.

(iii) All default passwords for accounts must be constructed in accordance with the PGF Password Policy.

(iv) Concurrent connections may be limited for technical or security reasons.

(v) All accounts must be disabled immediately upon notification of any employee's termination.

2.4.2 **Account Management**

(i) Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.

(ii) All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.

(iii) Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.

# 3. Hardware Policy

3.1 **PURPOSE**

The purpose of this policy is to provide a guidance for the procurement, management and disposal of all IT hardware for the PGF. The policy covers IT hardware purchases relating to the annual planning cycle, ad hoc purchases or upgrades of computer desktops, laptops, and peripherals.

This also to provide guidance and clarification of the policy and procedures covering the effective and safe use of PC or laptop computers issued to PGF employees.

3.2 **POLICY DETAILS**

3.2.1 **Procurement**

The procurement of laptops and desktops as part of the annual planning cycle will be under the budget of MIS Department and managed centrally by the PGF MIS Department.

PGF MIS Department will provide equipment that will allow staff to perform all their daily activities including complex spreadsheets, SAP, etc. As a default, all staff will be supplies with a windows laptop and associated peripherals as part of the replacement cycle.

The Standard provision for laptop user will include:

- Laptop and laptop bag
- Laptop adapter
- Wireless mouse
- An additional monitor if needed

The Standard provision for desktop user will include:
- Desktop CPU
- Monitor
- Keyboard and mouse
- An additional monitor if needed

Desktop or laptop specialist requirement outside of this speciation for 'High-End' or 'Power Users' will be reviewed on a case-by-case basis supported by a business case. Case will be reviewed by the PGF MIS Department.

3.2.2 **Deployment**

Laptop or Desktop will be configured, audited and deployed by MIS Department and will ensure that security procedure is followed when setting up software and hardware.

3.2.3 **Management**

The laptop or desktop will be tracked through use of the PGF MIS Asset Management database. All the MIS Asset will be allocated to named individuals. Any asset should not change ownership without the approval from the MIS Department.

3.2.4 **Replacement**

Desktop or laptop will typically have lifespan of 5 years, MIS Department will contact the named individual when the replacement of asset is due and approved by the management.

3.2.5 **Ad hoc purchase of desktop or laptop**

Any request for desktop or laptop outside of the planning lifecycle for example for new headcount, should made via email to PGF MIS Department.

## 4. Password Policy

4.1 **PURPOSE**

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords.

4.2 **SCOPE**

This policy applies to all PGF Employee who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any PGF facility, has access to the PGF network, or stores any non-public PGF information.

4.3 **DEFINITION**

**Password** - A string of characters which serves as authentication of a person's identity, which may be used to grant or deny access to private or shared data.

**Strong Password** - A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters,

depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the password owner such as a birth date, social security number, and so on.

4.4 **POLICY DETAIL**

4.4.1 **User Network Password**

Password for PGF network access must be implemented according to the following guidelines:

(i) Password must be adhered to a minimum length of 12 characters.

(ii) Password must contain a combination of alpha, numeric and special characters, where the computing system permits (!@#$%^&*_+=?/~';',<>|\).

(iii) Password must not be easily tied back to the account owner such as: username, IC number, phone number, nickname, birth date, etc.

(iv) Passwords must not be dictionary words or acronyms.

(v) Passwords cannot be reused.

4.4.2 **Password Protection**

(i) The same password must not be used for multiple accounts.

(ii) Password must not be shared with anyone. All passwords are to be treated as sensitive, confidential PGF information.

(iii) Password must not be inserted in e-mail messages or other forms of electronic communication.

(iv) Passwords must not be revealed over the phone to anyone.

(v) Passwords must not be revealed on questionnaires or security forms.

(vi) Users must not hint at the format of a password (for example, “my family name”).

(vii) Passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.

(viii) Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.

(ix) If suspect account has been compromised, the password must be changed immediately and report the discovery to the PGF MIS Department.

# 5. Email Policy

5.1 **PURPOSE**

The purpose of this policy is to establish rules for the use of PGF email for sending, receiving, or storing of electronic mail.

5.2 **SCOPE**

This policy applies equally to all individuals granted access privileges to any PGF information resource with the capacity to send, receive, or store electronic mail.

5.3 **DEFINITION**

5.3.1 **Gmail -** Email service provided by Google which is currently using by PGF.

5.3.2 **Antivirus** - Software used to prevent, detect, and remove malicious software.

5.3.3 **Electronic mail system** - Any computer software application that allows electronic mail to be communicated from one computing system to another.

5.3.4 **Electronic mail (e-mail) -** Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

5.3.5 **Inbound filters** - A type of software-based traffic filter allowing only designated traffic to flow towards a network.

5.3.6 **Quarantine** - Suspicious email message may be identified by an antivirus filter and isolated from the normal mail inbox.

5.3.7 **SPAM** - Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e- mail.

5.4 **LEGAL**

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Sending or forwarding internal discussion without permission
- Knowingly sending or forwarding an attachment that contains a virus

5.5 **POLICY DETAIL**

5.5.1 Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on PGF's computer systems. PGF can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by PGF, may be subject to open records requests, and may be accessed in accordance with this policy.

5.5.2 Incoming email must be treated with the utmost care due to the inherent information security risks. Gmail using anti-virus application to identify malicious

code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy.

5.5.3 Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed by Gmail from the email prior to delivery. Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered. Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

5.5.4 E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm PGF's reputation.

5.5.5 The following activities are prohibited by policy:

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.

- Using e-mail for conducting personal business.

- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.

- Violating copyright laws by illegally distributing protected works.

- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.

- Creating a false identity to bypass policy.

- Forging or attempting to forge e-mail messages.

- Sending or forwarding joke e-mails, chain letters, or hoax letters.

- Sending unsolicited messages to large groups, except as required to conduct PGF business.

- Sending excessively large messages or attachments.

- Knowingly sending or forwarding email with computer viruses.

5.5.6 E-mail is not secure. Users must not send passwords, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the PGF network without encrypting the data.

5.5.7 All user activity on PGF information system assets is subject to logging and review. E-mail usage is monitoring through Gmail admin portal.

5.5.8 E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of PGF, unless appropriately authorized (explicitly or implicitly) to do so.

5.5.9 Users must not send, forward, or receive confidential or sensitive PGF information through non-PGF email accounts. Examples of non-PGF e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, and e- mail provided by other Internet Service Providers (ISP).

5.5.10 E-mail for resigned staff

(i) Email accounts of resigned employees will be suspended at the end of the last working day.

(ii) Suspended accounts will be kept for 2 weeks before remove from the server.

(iii) Email will be download to archive if needed. Anyone that wish to check the archived will need to get permission from the resigned staff's HOD.

(iv) Anyone that wish to receive email send to the resigned staff will need to get permission from HOD.

(v) Housekeeping of archive email will be done every year, those emails that are no longer needed will be removed from the backup server.

(vi) HR will need to inform MIS department if staff resignation is confirmed. MIS department will then confirm with the resigned staff's HOD, is there a need to back-up a copy of resigned staff's email.

## 6. Internet Policy

6.1 **PURPOSE**

The purpose of this policy is to establish the rules for the use of PGF Internet for access to the Internet or the Intranet.

6.2 **SCOPE**

This policy applies equally to all individuals granted access privileges to any PGF information system or resource with the capacity to access the Internet, the Intranet, or both.

## 6.3 DEFINITION

6.3.1 **Internet** - A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

6.3.2 **Intranet** - A private network for communications and sharing of information that, like the Internet, is based on Transmission Control Protocol/Internet Protocol (TCP/IP), but is accessible only to authorized employees within an organization. An organization's intranet is usually protected from external access by a firewall.

6.3.3 **User** - An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

6.3.4 **PC** - It's either a desktop or laptop that is issued by company for work purposes.

6.3.5 **World Wide Web (www)** - A system of Internet hosts that supports documents formatted in Hypertext Markup Language (HTML) that contains links to other documents (hyperlinks) and to audio, video, and graphic images. Individuals can access the Web with special applications called browsers, such as Google Chrome

## 6.4 POLICY DETAIL

### 6.4.1 Accessing the Internet

Users are provided access to the Internet to assist them in the performance of their jobs. At any time, at the request of management, Internet access may be revoked. PGF MIS Department may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by malware. PGF will use internet filters to block high-risk content and deny access to any unwanted material or malware.

All software used to access the Internet must be part of the PGF standard software suite or approved by PGF MIS Department. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through a computer connected to PGF's network must do so through an approved Internet firewall or other security device. Bypassing PGF's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using PGF Internet access for: unauthorized access to local and remote computer systems, software piracy, illegal activities, the transmission of threatening, obscene, or harassing materials, or personal solicitations.

### 6.4.2 Expectation of privacy

Users should have no expectation of privacy in anything they create, store, send, or receive using PGF's Internet access.

Users expressly waive any right of privacy in anything they create, store, send, or receive using PGF's Internet access.

6.4.3 **File downloads and virus protection**

Users are prohibited from downloading and installing software on their PC without proper authorization from PGF MIS Department. Technical controls may be utilized to limit the download and installation of software.

Downloaded software may be used only in ways that conform to its license and copyrights.

All files, downloaded from the Internet, must be scanned for viruses using PGF approved virus detection software. If a user suspects a file may be infected, he/she must notify PGF MIS Department immediately.

Users are prohibited from using the Internet to deliberately propagate any virus, worm, Trojan Horse, trap-door, or other malicious program.

6.4.4 **Monitoring of computer and Internet usage**

All user activity on PGF MIS Department assets is subject to logging and review. PGF has the right to monitor and log all aspects of its systems including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

6.4.5 **Frivolous use**

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

6.4.6 **Content**

PGF utilizes software that makes it possible to identify and block access to Internet sites containing sexually explicit material or other material deemed inappropriate in the workplace. The display, storing, archiving, or editing of such content on any PGF PC is prohibited.

Users are prohibited from attempting to access or accessing inappropriate sites from any PGF PC. If a user accidentally connects to a site containing such material, the user must disconnect at once and report the incident immediately to PGF MIS Department.

# 7. Network Security and VPN acceptable use

## 7.1 PURPOSE

The purpose of this policy is to define standards for connecting to PGF's network from any host. These standards are designed to minimize the potential exposure to PGF from damages, which may result from unauthorized use of PGF resources.

Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PGF internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to DSL, VPN, SSH and etc.

## 7.2 SCOPE

This policy applies to all PGF employees with a computer or workstation used to connect to the PGF network. This policy applies to remote access connections used to do work on behalf of PGF, including reading or sending email and viewing intranet resources.

## 7.3 DEFINITION

7.3.1 **Virtual Private Network (VPN) -** A private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Some VPNs allow employees to securely access a corporate intranet while located outside the office.

7.3.2 **User Authentication** - A method by which the user of a system can be verified as a legitimate user independent of the computer or operating system being used.

7.3.3 **DSL** - Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

7.3.4 **Remote Access** - Any access to PGF's corporate network through a non- PGF controlled network, device, or medium.

7.3.5 **Split-tunneling** - Simultaneous direct access to a non-PGF network (such as the Internet, or a home network) from a remote device (PC, phone, etc.) while connected into PGF's corporate network via a Virtual Private network (VPN) tunnel. VPN is a method for accessing a remote network via "tunneling: through the Internet.

7.3.6 **IPSec Concentrator** - A device in which VPN connections are terminated.

7.3.7 **CHAP** - Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within

a user's access channel in a frame relay network and has local significance only to that channel.

## 7.4 POLICY DETAIL

### 7.4.1 Network Security

Users are permitted to use only those network addresses assigned to them by PGF MIS Department.

All remote access to PGF will either be through a secure VPN connection on a PGF owned device that has up-to-date anti-virus software, or on approved mobile devices.

Remote users may connect to PGF Information Systems using only protocols approved by PGF MIS Department. Users inside the PGF firewall may not be connected to the PGF network at the same time a remote connection is used to an external network.

Users must not install network hardware or software that provides network services without PGF MIS Department approval. Non-PGF computer systems that require network connectivity must be approved by PGF MIS Department.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, PGF users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the PGF network infrastructure. Only the PGF MIS Department is permitted to perform these actions.

Users are not permitted to alter network hardware in any way.

### 7.4.2 Remote Access

It is the responsibility of PGF employees with remote access privileges to PGF's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to PGF.

PGF employees are responsible to ensure that they:

- Do not violate any PGF policies
- Do not perform illegal activities
- Do not use the access for outside business interests

PGF employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of PGF's network:

- Virtual Private Network (VPN)
- Wireless Communications

7.4.3 **Requirements**

Secure remote access must be strictly controlled. PGF employees should never provide their login or email password to anyone, including family members.

PGF employees with remote access privileges:

- Must ensure that their computer, which is remotely connected to PGF's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

- Must not use non-PGF email accounts (i.e. Hotmail, Yahoo, Gmail), or other external resources to conduct PGF business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for split-tunneling or dual homing is not permitted at any time.

For remote access to PGF hardware, all hardware configurations must be approved by PGF MIS Department.

All hosts that are connected to PGF internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the PGF production network must obtain prior approval from PGF MIS Department.

7.4.4 **Virtual Private Network (VPN)**

The purpose of this section is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the PGF corporate network. This applies to implementations of VPN that are directed through an IPSec Concentrator.

This applies to all PGF employees, consultants, and other workers including all personnel affiliated with third parties utilizing VPN's to access the PGF network.

Approved PGF employees, may utilize the benefit of a VPN on a PGF device, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

The following guidelines will also apply:

(i) It is the responsibility of employees, with VPN privileges, to ensure that unauthorized users are not allowed access to PGF internal networks.

(ii) When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

(iii) VPN gateways will be set up and managed by PGF MIS Department.

(iv) All computers connected to PGF internal networks via VPN or any other technology must use up-to-date, anti-virus software applicable to that device or platform.

(v) To ensure protection from viruses, as well as protection of member data, only PGF-owned equipment will have VPN and Remote Access.

(vi) Only PGF MIS Department approved VPN clients may be used.

(vii) By using VPN technology, users must understand that their machines are an extension of PGF's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

7.4.5 **Support**

PGF will offer support for connectivity to the PGF network. PGF is not responsible for ISP outages that result in a failure of connectivity to the PGF network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the PGF network.

## 8. Anti-virus

8.1 **PURPOSE**

This policy was established to help prevent infection of PGF computers, networks, and technology systems from malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

8.2 **SCOPE**

This policy applies to all computers connecting to the PGF network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment connecting to the PGF network.

8.3 **DEFINITION**

8.3.1 **Virus** - A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

8.3.2 **Trojan Horse** - Destructive programs, usually viruses or worms, which are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or removable media, often from another unknowing victim, or may be urged to download a file from a web site or download site.

8.3.3 **Worm** - A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

8.3.4 **Spyware** - Programs that install and gather information from a computer without permission and reports the information to the creator of the software or to one or more third parties.

8.3.5 **Malware** - Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

8.3.6 **Adware** - Programs that are downloaded and installed without user's consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exception after installing.

8.3.7 **Keyloggers** - A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via email).

8.3.8 **Ransomware** - A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid.

8.3.9 **Server** - A computer program that provides services to other computer programs in the same or other computers. A computer running a server program is frequently referred to as a server, although it may also be running other client (and server) programs.

8.3.10 **Security Incident** - In information operations, a security incident is an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

8.3.11 **E-mail** - Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

8.4 **POLICY DETAIL**

All computer devices connected to the PGF network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

The virus protection software must not be disabled or bypassed without PGF MIS Department approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server, attached to the PGF network, must utilize PGF MIS Department approved virus protection software and setup to detect and clean viruses that may infect PGF resources.

All files on computer devices will be scanned periodically for malware.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the PGF MIS Department.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the PGF network until the infection has been removed.

## User should

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from Bin.
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Always scan removable media from an unknown or non-PGF source (such as a CD or USB from a vendor) for viruses before using it.
- Back up critical data on a regular basis and store the data in a safe place. Critical PGF data can be saved to network drives and are backed up on a periodic basis. Contact the PGF MIS Department for details.

Because new viruses are discovered every day, users should periodically check the Anti-Virus Policy for updates. The PGF MIS Department should be contacted for updated recommendations.