PGi IT Security Statement

April 2020

Table of Contents

Introduction

PGi maintains an information security program that passes a SOC 2 Type 2 Audit annually covering the Security Confidentiality and Availability Trust Principles.

PGi's senior management has issued an Information Security Policy, which is a guiding framework for all security processes and procedures. The policy is the cornerstone of PGi's information security program and aims to secure PGi's information assets.

The objectives are:

- Protect PGi's information assets and those of its clients from internal and external threats
- Ensure the maintenance of confidentiality and availability of information
- Meet statutory, regulatory, and contractual obligations
- Grant access to information assets only for specific business needs
- Identify and hold accountable individual users of information assets while potentially monitoring their use of those assets

This document provides a summary overview of the IT security controls employed by PGi. It can be shared with current and potential clients.

Information Security Organization

Internal Organization

PGi's IT organization has a dedicated Information Security group, led by its Vice President of Information Security. This group works closely with PGi's Chief Technology Officer, Finance Department, Legal Department, and business representatives to enable identification of information risks. PGi must appropriately address those risks to meet legal, regulatory, and contractual obligations.

In addition, a leading Security Managed Services Provider is a dedicated Security Operations Center to achieve secure daily IT operations.

Authorization Process

The IT organization has a request process guiding the introduction of any new hardware and software.

Confidentiality Agreements

All PGi's employees and contractors (“Associates”) are required to sign non-disclosure agreements as a condition of hiring.

External Party Access

PGi protects its information and technology assets against risks created by external party access (for example, suppliers) or as a result of the outsourcing of services with the following guidelines:

- Adequate security controls must be defined and implemented.
- Third party logical access to PGi information and systems must be authorized by the owner of the information or systems.
- Security controls must be put in place, restricting the third-party access to information and systems that are required for them to perform the service specified in their contract of engagement with PGi.
- Third parties contracting with PGi who require access to PGi IT resources must agree in writing to adhere to the relevant PGi information security policies.

- Access to personal data requires the third party to fulfill the requirements of PGi and relevant regulations.
- An authorized individual from the third party must sign, on their behalf, a data processing agreement before PGi granting the third-party access to PGi information or systems.

Resource Management

Resource Inventory and Classification

PGi's IT organization has an asset inventory process for information assets (data, applications, and physical assets). This process includes:

- Determination of the sensitivity level of information assets
- Identification of the information and application owners
- Identification of disaster recovery requirements (in other words, recovery point and recover time objectives)
- Identification of security risk factors and corresponding security controls

Data Security

Customers accessing PGi applications are limited through the application to view only their own data. Within their IDs, customers can further segment rights for their own employees.

All PGi products are designed with security from the ground up and PGi software developers routinely audit code during the development cycle.

PGi employs strong encryption for transmitting sensitive information across the network. This includes the use of Transport Layer Security (TLS) for web-based communications, to protect customer credentials and communications.

PGi runs quarterly audits of the Microsoft network to verify what permissions have been granted and revoke any permission which does not fall into the permissions policy.

Application Security

PGi maintains multiple layers of hardware and logical access controls to protect the integrity and the confidentiality of resident customer data. We have developed a platform that is adaptable to internal and external security requirements. Elements of our security infrastructure include:

- Firewalls (including cloud security gateways) to manage Internet access using port and rule-based controls. All back office data is held secure within the PGi network or cloud infrastructure.
- All web interfaces and components are hosted on secure servers with SSL certificates and all web servers reside behind a secure firewall architecture.
- Intrusion Detection Systems (IDS) are used to monitor and detect unwanted activity.
- ID Management through an LDAP /Kerberos-based authentication for production systems.
- Internal and external vulnerability scans are performed routinely by the Information Security team and annually by a qualified third party. Vulnerabilities are analyzed and then remediated.
- Antivirus protection on user desktops and production systems that run the Windows™ operating system.
- Use of a private WAN between our production centers with multiple links between core sites using multiple carriers on each leg. We use OSPF so if any one links fails there is no interruption to service.
- PGi has primary and secondary firewalls on our ISP connections.

Information Handling

To secure information properly, PGi applies handling controls that are appropriate to the requirements and sensitivity of the information. Examples of these controls include:

- Information owners must ensure that data destruction, retention, and backups comply with business, legal, and regulatory requirements.
- Authentication and authorization technologies control internal access to information. PGi has processes in place to grant only the minimum access permissions required for each authorized user's role to perform his or her job function.
- All assets owned by PGi and used by individuals such as employees, contractors, and third parties are to be returned upon termination of employment, contract, or agreement.

- Except for checking email, PGi information is not stored, processed, or transmitted by PGi Associates on equipment which is neither managed nor owned by PGi. The external equipment includes personal home computers and other mobile computing devices such as smartphones.
- PGi follows a disposal policy for secure media destruction. Any media are irrecoverably erased or physically destroyed in accordance with recognized best practices before disposal.
- All PGi products are served from telco-grade facilities. The switches, bridges, servers, computer network, office computers, and peripherals are in facilities that provide the highest levels of protection for:
  - **Power** – with the provisions Uninterruptable Power Supplies, backup generators and separate A and B power distribution to each equipment rack
  - **Cooling** – provision of at least N+1 cooling system in each facility
  - **Carriers** – data centers are selected based on access to multiple telecommunication carriers from within the facility

Redundancy and Resilience

One of PGi's greatest strengths is its site diversity and global presence. PGi's products are built with high availability in mind with equipment redundancy and layers of application and database redundancy built in.

Audio bridging platforms are deployed in configurations with redundant audio bridges in each node. IP bridge configurations allow the removal of a failing bridge from service and the others in that node automatically take up those conferences. Application and web-based infrastructure generally consists of multiple instances running on server clusters together with VM technologies to provide the highest levels of redundancy and availability.

PGi's carrier network for voice access is designed around multiple carriers with separate toll and toll-free numbers in many geographies.

Nightly backups of all core systems are taken, and databases are replicated in real time. Initial backups are taken to disk and these are then transferred to disk offsite at secure facilities. Inventory lists are maintained to allow for immediate recovery in the event of a disaster.

Human Resources Security

Prior to Employment

All newly hired personnel must have background/reference checks as appropriate, permitted, and customary depending upon the Associate's location. All new Associates must also agree to abide by professional standards, data privacy legislation, and PGi's policies regarding information security, appropriate usage, and business ethics.

Temporary or contract Associates must go through the same vetting processes as regular Associates. Where their recruitment has been sub-contracted to a third party, our contract with the third party must clearly state these requirements.

Security Responsibilities

Associate responsibilities for information security are defined and communicated through training and security policies. Furthermore, Associates must complete annual training to provide adequate knowledge regarding information security, data protection, and their corresponding responsibilities. All Associates receive communications about their information security responsibilities through Intranet posts, flyers, or emails.

Security Awareness

Security and Privacy awareness training is annual. In addition, all Associates receive communications about their information security responsibilities through Intranet posts, flyers, or emails.

Termination Processes

Access rights of all employees, contractors, and third parties to PGi's internal systems, applications, and infrastructure are revoked upon termination of employment, contract, or agreement. They are amended appropriately upon any change of roles.

Physical and Environmental Security

Security Controls

Examples of the security controls which are in place within PGi premises (where confidential data is processed) and those of our subcontractors are:

- The security perimeters for such buildings must be well defined and physically sound. External doors of PGi areas must be suitably protected against unauthorized access.
- All building visitors must sign a visitor's book when entering a building where confidential data is processed. Except for publicly accessible/open areas, all visitors are to be escorted by an Associate.
- PGi issues staff identification cards to all Associates. The associates must visibly wear the identification cards when they enter a PGi building.
- Only Associates who have authorized permission are allowed access to all premises.
- Visitors requiring access to secure areas, such as information processing centers, who have not been vetted are always escorted by an authorized Associate. In addition, they must record their access in a visitor/vendor tracking book.
- A clean-desk directive applies throughout the organization. Confidential information must be locked away outside office hours.

Physical Controls

The physical and environmental controls incorporated into the design of the PGi data centers are:

- The distance between primary and secondary data center is far enough to prevent both data centers from being affected by a disaster at the same time
- Burglar alarm system
- Temperature and humidity control and monitoring
- Smoke detection alarm
- Lightning and transient voltage suppression
- Redundant power feeds
- Generator-backed UPS systems
- Physically separated PGi areas with dedicated access controls. Data center access is limited to authorized personnel. Visitor access procedures are established

Communications and Operations Management

Operational Procedures and Responsibilities

The PGi IT organization has established and maintains procedures. Roles and responsibilities are defined and include appropriate segregation of duties to prevent both fraud and potential malicious or accidental misuse of the systems.

Patch Management

Appropriate patch management processes relating to vendor patches and fixes are in place. Patches released are tested and applied on a schedule suited to the actual risk to achieve protection from vulnerabilities.

Capacity Management

A capacity management process is in place and capacity reports are reviewed regularly by PGi's IT organization.

Development and Stage Environments

For critical systems, PGi maintains separate development, stage/test, and production environments.

Network Perimeter Security

Firewalls (including cloud security gateways) protect PGi's network perimeter and, where appropriate, intrusion detection systems (IDS). The firewalls and IDS event logs are correlated and monitored 24x7 for unauthorized access attempts or other kinds of attacks by a Managed Security Services provider.

For Internet-accessible applications, a tiered network design is implemented in the Internet-DMZ. The three tiers (load balancers and reverse proxies, web and application servers, and database servers) are separated and secured from each other, the internal PGi network, and the Internet by firewalls.

Internal Network Security

For internal servers and applications, intrusion detection systems (IDS) are located at strategic locations in the WAN network. The firewall and IDS event logs are correlated and monitored 24x7 for unauthorized access attempts or other kinds of attacks by a Managed Security Services provider. All urgent issues and alerts are escalated through the NOC (Network Operations Center). Additional technical and management resources are immediately engaged as needed. An operations manager is available 24x7 to manage any escalation that may be required.

Network devices, routers, diagnostic equipment, and other equipment are physically secured in access-controlled areas, accessible only by authorized PGi Associates.

Wireless Networks

Access to PGi's wireless networks requires authentication (valid username/password), and connections are encrypted using 128-bit SSL.

Remote Access

PGi provides employees with a virtual private network (VPN) to enable secure, Internet-based remote access. Creating a VPN tunnel requires a two-factor authentication (valid username/password and separate electronic token or SMS message). VPN tunnels are secured using strong encryption.

PC Security Software Suite

PGi uses a software combination to provide a secure computing environment. PGi has adopted the industry practices associated with recognized global standards to ensure the security and integrity of our systems.

- **Antivirus** – All PGi's PCs are equipped with a mandatory virus protection software that performs on-access scans of all data. The software is configured to clean or delete infected files. Antivirus signatures are updated at least daily.
- **Personal Firewall** – PGi's personal firewall software is automatically enabled and uses a standard configuration to protect against malicious network traffic, including Internet-based network threats, non-trusted networks, or malicious software. Base configuration settings are secured against change, tampering, or disablement by end users or malicious programs.
- **Secure Remote Access** – PGi utilizes virtual private network (VPN) software, configured to require two-factor authentication and strong encryption, to enable secure remote access to PGi networks.
- **Screen lock** – Password protected screensavers, which activate after a period of inactivity, are used where operable.
- **Systems Management Software** – PGi uses a software management process to update its PCs with all applicable security patches.
- **Microsoft Office 365** – PGi uses Microsoft Office 365 for several applications, including email. PGi uses two-factor authentication to access the applications.

Server Operating System Controls

Servers are configured with standard images that incorporate security controls, including antivirus software for Windows systems.

Penetration Testing

A third party annually performs a penetration test. Any issues found through the penetration tests are corrected within a timeframe corresponding to the problem's actual risk.

Payment Card Handling

PGi maintains Payment Card Industry (PCI) compliance and regularly audits the card handling areas to verify that all facilities in scope comply with the major Card Associations' published security guidelines and requirements.

Vulnerability Scans

Automated vulnerability scans are performed on a monthly basis. Weaknesses identified by these scans are corrected within a timeframe corresponding to the actual risk.

Audit Logging

PGi maintains audit logs for servers, applications, and network devices that record the occurrence of system faults and security events and facilitate examination of abnormal activities. Logs are reviewed as required, either manually, reactively, or by a real-time security event monitoring system.

System Backup

Server systems are backed up daily.

- Operational procedures verify the successful completion of backups.
- Backed-up data is stored in a secure, fire-protected location.

Secure Storage Media Disposition

Procedures are in place for the secure erasure (using multiple random overwrites or equivalent) or destruction (degaussing or shredding) of storage media (hard drives, back-up tapes, and so forth) prior to disposal.

Web Access Security

PGi has deployed real-time web access security software that blocks access to insecure and inappropriate web sites from the PGi network.

Spam Blocking and Email Threat Protection

PGi has established and maintains email gateway spam-blocking and antivirus software. Threat protection is used to minimize threats from impersonation attempts, phishing, or email-borne malware.

Access Control

Authorization and Authentication Controls

Authentication and authorization technologies control access to IT resources. PGi follows a process to grant or revoke access to IT resources. Access is based on the principle of least-privilege by role. Least privilege means that a user has only the amount of privilege that is necessary to perform a job.

PGi has established procedures for creation, amendment, and deletion of user accounts for Associates, including processes to disable or delete accounts for terminated personnel. All PGi Associates are required to agree to take reasonable precautions to protect the integrity and confidentiality of security credentials.

Privileged Access

Privileged access (for example, “administrator” or ”root”) is limited to essential PGi administration personnel. Associates with privileged accounts are to use a separate, non-privileged account for performing normal business functions.

User Accounts and Passwords

Passwords protect user accounts. Periodic password changes, a minimum password length, password complexity, and limitations for password reuse are enforced by policies and, where possible, by technical measures. User accounts are locked for a predetermined period after a set number of failed login attempts to prevent brute force password attacks. It is not permitted to divulge passwords.

Information Systems Acquisition, Development, and Maintenance

PGi has established a process to manage systems acquisition, development, and maintenance. Key security-related components include:

- A documented systems development life cycle with appropriate reviews and scans
- All outsourced software development is supervised and monitored appropriately
- Change management procedures are established and followed
- Separation of duties

Information Security Incident Management

PGi has established an Information Security Incident Response process and documented procedures for managing security incidents. The incident response process is:

1. **Discovery and notification** – All PGi employees and its contract partners are to notify PGi's Information Security Team immediately if an information security incident or vulnerability is observed or suspected.
2. **Initial assessment** – PGi's Information Security Team decides, depending on the type and circumstances of the event, the potential damage, and whether further escalation is required. Any mitigating measures that should be deployed immediately, are identified and implemented.
3. **Escalation** – Involvement of the relevant persons/instances.
4. **Deployment of damage-limitation measures** – Measures appropriate to stop the incident or to minimize the damage are identified and implemented.
5. **Determination of cause and securing evidence** – The causes or triggers and exact circumstances of the incident are determined, and evidence is collected and secured.
6. **Recovery** – The damage/consequences caused by the incident and all problems that might have facilitated the incident are resolved.
7. **Post-processing** – If appropriate, criminal, civil or employment law measures are taken. measures appropriate to prevent a repetition of the incident are defined.

Business Continuity Management

PGi maintains an IT Business Continuity Plan. The purpose of this plan is to establish procedures for counteracting interruptions to business activities and reducing the impact caused by disasters or other significant events. Planning includes both preventive and remedial measures.

The following points summarize the most important details regarding PGi's Business Continuity Plan:

- Based on impact analyses, appropriate maximum acceptable data loss and recovery time in case of a disaster are determined. Appropriate technical and organizational measures are implemented to fulfill the requirements.
- PGi uses multiple data centers. The distance between data centers is far enough to prevent more than one from being affected by a disaster at the same time.
- An IT crisis management organization with corresponding roles and responsibilities has been established.
- Emergency escalation and restoration procedures have been documented and are periodically updated.
- Appropriate data is backed up on a regular, automated schedule. In addition, critical data is mirrored to storage in other data centers.

Compliance

Compliance checks support compliance with PGi's security policies. These compliance checks include:

- Annual SOC 2 Type 2 audits of our products and environment performed by an external auditor.
- Vulnerability and compliance scans for sensitive server systems, server-based applications, and network devices.