PGi Your Partner in Collaboration

Security, Resilience & Continuity

Contents

Meetings and Collaboration

PGi is a leading global provider of advanced meeting, conferencing and collaboration solutions. We have a global presence in 24 countries and an established base of more than 45,000 customers, including nearly 75% of the Fortune™ 500. Every month, we facilitate 3 million virtual group meetings with more than 12 million participants worldwide.

This document provides an overview of PGi's commitment to system security, integrity and business continuity, specifically designed for our Global Meetings and Collaboration services.

Application Security

PGi is committed to protecting the privacy of every client we serve. Dedicated security protocols throughout our system ensure sensitive client information remains private. From encryption technology where warranted, and industry-leading conference security features, to an advanced fault-tolerant redundant architecture, PGi delivers some of the highest levels of security in the industry

Our automated audio conferencing offerings provide a number of security features built in:

- A separate moderator passcode to ensure only the moderator can initiate the call
- Conference lock to prevent anyone from joining after the meeting begins
- Moderator-controlled roll call to let the moderator know at any time who is in the conference
- Availability of ten-digit random passcodes for additional security
- Optional web based controls that enable the moderator to instantly mute lines, disconnect callers, adjust volume, eliminate line noise, and dial out, all at a keystroke from the desktop tones on entry/exit to notify others on the call when a participant joins or leaves
- On-hold music for participants until the moderator is ready to begin the conference

PGi's Online Admin Portal is a website providing a central management framework for your customer administrator to organize and access your organization's audio, video, web, and event conferencing services. Through the Online Admin Portal web interface, administrators can:

- Create and manage moderator and participant accounts
- Set meeting preferences
- Track participations
- Change and generate moderator and conference passcode
- Activate enhanced security features, such as:
    - 10-digit random passcodes
    - Music on hold
    - Activity reporting
    - Access recordings

Physical Security

All areas deemed to contain sensitive data, or where our production systems and audio bridges are located, are locked, with access only provided to authorized employees.

To ensure a secure physical environment, PGi limits all facility access based on business needs in accordance with job responsibilities. Each employee's role is evaluated before access levels are assigned. Non-operational staff may only access a data center with an approved escort. Access is monitored through auditing and logging, and alert tools keep management aware of violations or exceptions.

Our production conference bridges are maintained in secure co-location or cloud services facilities where only authorized staff may have access. All visitors to these facilities must be accompanied by an authorized staff member and all visitors require pre-clearance in advance of arrival. Cage access histories are recorded and reviewed.

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 to manage Internet access using port and rule-based controls. All back-office data is held secure within the PGi network or cloud insfrastructure.
- All web interfaces and components are hosted on secure servers with SSL certificates and all web servers reside behind a secure firewall architecture.
- The implementation of multiple ISP internet connections, using BGP routing and a PGi-assigned IP range, so that PGi is not reliant on any one ISP.
- Intrusion Detection Systems (IDS) are used to monitor and detect unwanted activity.
- ID Management via an LDAP /Kerberos-based authentication for production systems.
- Network Vulnerability Scans. Internal and external scans are performed routinely by the Information Security team and annually by a qualified third party. Vulnerabilities are analyzed then remediated.
- Anti-Virus Protection on user desktops and production systems that run the Windows™ operating system.
- Use of a private WAN between our production centres 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.

Data Security

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

All PGi products are designed with security from the ground up. 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.

We run quarterly audits of our Microsoft network to verify what permissions have been granted, and we revoke any permission which does not fall into our permissions policy.

Employee Access

Employee access to all PGi system utilities are based on business need in accordance with job duties and responsibilities. PGi employs a formal procedure for granting, modifying and revoking access to all information, systems and networks. Contractors and third-parties (e.g., external service providers) may access PGi information systems based on business requirements and subject to PGi management approval. Access is granted only for the time required to accomplish defined and approved tasks.

Remote access to PGi's internal network by authorized users (e.g., staff working remotely) requires multifactor authentication in addition to User IDs and passwords. Access is granted through virtual private network (VPN) that provides encryption and secure authentication.

Redundancy and Resilience

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

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

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

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

Data Center Redundancy

All PGi conferencing facilities are located in telco-grade facilities. The switches, bridges, servers, computer network, personal computers and peripherals are located 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 systems in each facility
- Carriers – our data centers are selected on the basis of access to multiple telecommunication carriers from within the facility

PGi also adds the protective measure of provisioning redundant facilities with reserve processing capacities, including local and off-premises backups of essential information.

Business Continuity

PGi has a business continuity program to provide oversight to continuity and recovery preparation efforts. PGi maintains plans for keeping operations running in the event of disasters or other events. The BC program includes keeping the plans up-to-date as well as conducting annual tests of the recovery capabilities.

Audits and Standards

PGi has adopted the industry practices associated with recognized global standards to ensure the security and integrity of our systems. PGi uses EU Standard Contractual Clauses to legally process personal data.

PGi regularly conducts penetration audits via an external company to test PGi's external network and identify possible exposures. Industry-accepted network testing tools and manual penetration techniques are used to assess the protection surrounding PGi Internet-facing resources.

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.

Management

PGi management has a strong, ongoing commitment to ensuring our systems are secure and always available to meet our customer's needs.

Network Operations Centre

PGi operates a 24x7 Network Operations Centre which monitors our global infrastructure through operations software (for example, Orion). All issues and alerts are escalated through the NOC. Additional technical and management resources are immediately engaged as needed. An operations manager is available 24x7 to manage any escalation that may be required.

Change Control Practices

PGi uses a change management practice for any alterations to the production network, and hardware or software components. All changes are reviewed and approved prior to deployment.

Ongoing Risk Assessment

PGi constantly evaluates various risk scenarios which could impact security, system infrastructure, or impede operations and standards compliance. Management actively promotes programs for ongoing risk assessment and reduction, and supports the development and maintenance of necessary procedures and product standards needed to keep current with evolving issues.