Park City Group
Advanced Commerce – Security Overview

Park City Group (PCG) is a leading provider of Advanced Commerce solutions for the CPG (Consumer Packaged Goods) and other industries. Our services include basic data synchronization between suppliers and retailers, as well as advanced services such as Scan Based Trading (SBT), Visibility & Analytics (V&A), and Scan Sales Invoicing (SSI).

These and other Park City Group services involve the import, processing, and export of data between client trading partners. Both informational data, such as item and cost records, and transactional data, such as delivery and sales receipts, are handled through our Advanced Commerce application.

Because this data is sensitive and proprietary to each of our clients, highly structured security policies are in place that are rigidly enforced for each aspect of our operations.

This document provides a *high-level overview* of the basic elements of our policies.

Client User Security

A client user represents a company subscribing to Park City Group services. Users log on to specific accounts within the Advanced Commerce application to manage data on behalf of the client.

Client User Access

To maintain the integrity and confidentiality of client data, no client user has direct access to the Advanced Commerce database. Instead, all visibility and updates occur through our "batch" and "online" applications. This limits user access to only those areas in which a client company has been granted authorization. Park City Group maintains an activity log of each user's online and batch transactions.

Client Usernames and Passwords

Usernames and passwords are required for access to Park City Group's online application. Each new user is assigned a temporary password that must be changed the first time they log on. Security policies dictate the length and format of passwords, as well as providing long-term restrictions limiting when a previous password can be reused. Client passwords expire every 60 days, requiring the user to enter a new password after this time has elapsed.

In addition, each user is required to select and answer a security question the first time they log on. For example, *What's your favorite Pet's Name?*

Should a user forget his or her password, they can request a temporary password online after providing validations that include the user's security question / answer. The user's Client Security Administrator can assist with this process. Temporary passwords are sent to the e-mail address on file, and must be changed at the next log on. A user's account is *locked out* if someone with a current username attempts to log on three times with an incorrect password.

Authorizations

Authorizations limit client user access to only those areas necessary to maintain the day-to-day operations for their company in Park City Group. These can range from simple view only or update access to administrative and report-distribution privileges.

Client Security Administration

Each company that subscribes to Park City Group selects a member of their staff to serve as an onsite Client Security Administrator. This allows clients to internally manage their own user's access. Security Administrators can assist users in resetting passwords and managing personal information, such as e-mail addresses and telephone numbers stored in the application. Security Administrators can also grant or rescind user authorizations within their company.

Note: Security Administrator privileges are limited to managing users within their own organization. No Administrator can access another client's account, and policies are in place to prevent access by a former Administrator relieved due to termination or a change in responsibilities.

Associate User Security

An associate user is a Park City Group employee authorized to perform tasks in support of Park City Group's Advanced Commerce application. Each associate's access to client data is limited by the authorizations and other policies briefly described below.

Associate Usernames and Passwords

Username and password rules for associates are identical to those of client users, including password length, format, expiration, and selecting/answering a security question. The primary difference between associate and client user security is in the *authorizations* granted to associates, as described below.

Authorizations and Data Visibility

Park City Group applications provide internal authorization levels that control associate access to client data and system functions. Each associate's access is limited to just those areas needed to perform his or her assigned duties. As such, only associates in support and implementation positions can view a client's item, cost, and transactional data. Only Operations personnel have direct access to the Advanced Commerce database.

VPN and other controlled access

Associate access to Park City Group's application infrastructure and internal network takes place through a VPN (virtual private network). Transmissions over the VPN are encrypted, and require username/password validation separate from that used in basic application access. Direct access to the database is limited to key individuals.

New Hires / Terminations

Strict security procedures are followed whenever a new associate is hired or an existing associate leaves Park City Group. These procedures include adjusting network and application access, as well as the assignment / recovery of laptops, access cards, and other sensitive materials.

Infrastructure Security

This section outlines the security policies in place for Park City Group's Advanced Commerce infrastructure, including physical and network security, change control, quality assurance, and support. This is a high-level overview only.

Physical Security, Reliability, and Backup

Our Production environment is located in a fully equipped hosting facility servicing some of the largest global organizations. This facility is completely secure, environmentally controlled, and fully redundant. It is staffed and monitored 24 hours a day, 365 days a year to ensure that all clients' critical daily processes run smoothly and efficiently.

Network Security

Park City Group's network security is designed and implemented around "quarantined areas." This approach uses secure checkpoints for access authorization and provides for layered intrusion detection. Each area is comprised of redundant servers to ensure scalability and availability, and is "blocked off" from all but other known authorized systems.

Security Testing and Maintenance

Park City Group performs quarterly reviews to reevaluate our security and determine if OS (operating system) upgrades are required. New security patches are installed as needed.

Code Change Controls

Park City Group utilizes a controlled, structured process for making changes to our application code. This process provides a methodology for clients and associates to request enhancements, updates and fixes to the Advanced Commerce application. All requests go through a multi-level review process before code changes begin. The coding process limits who can make changes to each area of the application, and includes code reviews and QA (quality assurance) testing.

Quality Assurance

Extensive testing of all code is performed before releasing it to our Production environment. Day-to-day operational monitoring and communications from Client Support supplement this testing in real world situations. If defects are found, QA works with the Development team to correct the "bug", perform testing, and apply changes quickly and efficiently.

Park City Group Support Teams

In addition to every associate playing a support role, three distinct teams are set up to provide assistance and monitoring.

- **Product Support** provides direct product assistance to clients. This is available through a toll-free number, via e-mail, and through Park City Group's online Feedback option.
- **Operations Support** monitors system availability and performance. Designated "On Call" associates perform this service 24 hours a day, 365 days a year. This position serves as a supplement to the monitoring provided by our offsite hosting facility.
- **Development Support** provides application and code assistance to Client Support and Operations Support, and is available 24 hours a day, 365 days a year.

Outage Communications

In the event of a *planned outage*, clients are notified by e-mail at least 30-days in advance, with follow-up telephone calls to client IT (Information Technology) departments for those clients whose inbound / outbound transactions might be adversely affected.

Unplanned outages are corrected as soon as possible to minimize any adverse effects. If an unplanned outage will last more than a few hours, clients are notified via e-mail with follow ups to key IT departments.

Data Retention

Within Park City Group's applications, data is classified into specific categories, with each category having its own retention policy. This policy is used to purge data once its category's time-based "aging" limitations are reached. A copy of our current policy is available upon request.