



PI Worldwide[®]

Hosting and Data Security Policy

**PI Worldwide
16 Laurel Ave
Wellesley, MA 02481
781-235-8872**

PI Worldwide[®], Predictive Index[®], *accessPI*[™] and *accessPI-CONNECT*[™] are registered trademarks and trademarks of Praendex Inc., doing business as PI Worldwide, in the United States and other countries. Any use without the express written consent of Praendex Inc. is strictly prohibited.

1. INTRODUCTION

This Hosting and Data Security Policy (“Policy”) describes the guiding principles, policies and best practices used by PI Worldwide (“Company”) with respect to the protection and security of the data that clients of Company and its licensees (“Clients”) store in Company systems such as *accessPI*[™] or otherwise provide to Company (“Client Data”). Company has adopted this Policy in order to demonstrate its compliance with the undertakings Company and its licensees make in agreements with Clients and in accordance with Company’s published Product User Privacy Policy.

This Policy addresses broadly all aspects of maintaining a secure environment at the Company as it relates to the protection of Client Data. The purpose of this Policy is to establish administrative, technical and physical safeguards for Client Data that are appropriate to: (a) the size, scope and type of business of the Company; (b) the resources available to the Company; (c) the amount of Client Data stored by the Company; and (d) the need to ensure that the Company’s Client Data is secure and maintained in confidence. A primary goal of this Policy is to cause everyone with access to Client Data to continually assess the security and confidentiality of information that we handle at the Company and apply reasonable safeguards to protect that information from unauthorized access. The Company’s policies, procedures and practices have been designed to meet these goals.

2. GENERAL GUIDELINES

The Company has adopted the following general guidelines for the handling of Client Data.

(1) **Be attuned to the Client Data in your environment.** Everyone should use good judgment to make sure that Client Data is secure. Avoid discussing Client Data where it can be overheard by unauthorized individuals, such as in the office lobby or other public areas. Papers, documents, computers and storage devices containing Client Data should not be left unattended in public areas. When you will be away from your work area for an extended period of time, Client Data should be stored in locked cabinets, drawers or containers.

(2) **Take reasonable steps to keep Client Data secure and confidential.** Everyone should continually assess the way they handle Client Data and select reasonable methods to secure it against loss, theft or unauthorized access. The Company’s policies outline a number of specific steps you should follow, but you should always exercise common sense and good judgment.

(3) **Do not transport or send Client Data outside of the Company without taking appropriate security precautions to protect it against loss, theft or unauthorized access.**

(4) **Be aware of visitors.** All employees must be vigilant if there are visitors to Company offices or facilities. All visitors who are provided access to Company computer systems or sensitive

areas, such as the Company's data centers or files containing Client Data, must be supervised by authorized personnel at all times.

(5) **Securely dispose of Client Data when retaining it no longer serves a legitimate business purpose or is required by law or Client agreements.** Client Data cannot simply be thrown away. It must be destroyed so that it cannot be read or reconstructed later by someone who obtains access to the Company's trash or to discarded computers or storage devices. When disposing of Client Data, physical documents must be redacted or shredded so that the Client Data cannot be practicably read or recovered. Similarly, electronic files and any disk or device containing Client Data must be securely disposed of to prevent recovery of the Client Data.

(6) **If you become aware of a potential breach of security or the loss or theft of Client Data, report it immediately to a member of the Data Security Committee, whose members are Mary Beth Cotter and Harry Moulis.** The Committee shall investigate and take prompt emergency action to prevent harm, avoid liability, and prevent the destruction of evidence. The Committee shall provide the Chief Executive with a report documenting the incident and responsive actions taken or to be taken in connection with the incident.

(7) **Consult the Data Security Committee about data access needs.** In the event that a legitimate need to access Client Data arises beyond the circumstances enumerated in this Policy or the Company's policies and procedures, including when the Company receives subpoenas, compulsory legal process and other requests, the Committee shall be consulted and provide written consent before access to Client Data is granted.

(8) **There are consequences to violations of this Policy.** Violations of this Policy, including careless, accidental or intentional disclosures of Client Data, may result in disciplinary action, up to and including immediate termination of employment or all existing business relationships with the Company. Violators may also be subject to civil or criminal liability. The Company will evaluate the appropriate disciplinary measures and legal actions on a case by case basis.

3. GENERAL SYSTEM INFORMATION

System Name/Title

- *accessPI*[™] - accesspi.piwebservices.com
- *accessPI-CONNECT*[™] - connect.accesspi.piwebservices.com

General Description/Purpose

- ***accessPI* (accesspi.piwebservices.com):**
Internet based on-line management tool that enables Predictive Index[®] customers to administer *PI*[®] Surveys and *PRO*'s and perform other useful functions, such as comparing, creating reports, etc. In addition, clients manage their data – saving, deleting and organizing all data they store in *accessPI*.
- ***accessPI-CONNECT* (connect.accesspi.piwebservices.com):**
Internet based application interface web service that enables the applications and web

sites of Predictive Index customers and partners to administer PI Surveys through their application and to view those PI Surveys from within their applications.

4. ADMINISTRATIVE RESPONSIBILITY

Company's Data Security Committee, currently Mary Beth Cotter and Harry Moulis, are responsible for developing and monitoring our security efforts, investigating potential threats, overseeing the Company's information security training program and establishing best practices. The Committee's responsibilities include:

- (1) Developing, implementing, administering and maintaining this Policy and any policies and procedures necessary to effectuate this Policy.
- (2) Assessing and identifying reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of Client Data.
- (3) Evaluating and improving, where necessary, the effectiveness of the Policy and the Company's safeguards for limiting risks to Client Data.
- (4) Designing, implementing and overseeing ongoing employee training and awareness programs.
- (5) Managing and responding to incidents involving information security, such as breaches or potential breaches involving Client Data or violations of this Policy. The Committee will also be responsible for documenting the Company's response to incidents and recommending changes to this Policy or the Company's business practices.
- (6) Overseeing the Company's relationships and contracts with third party service providers to ensure the security of Client Data.

Contact Information:

Name: Harry G. Moulis
Title: Associate Director, Applications and Technology
Company: PI Worldwide
Address: 16 Laurel Ave.
City: Wellesley, MA 02481
Phone: 781-235-8872
E-mail: hmoulis@piworldwide.com

Name: Mary Beth Cotter
Title: Contracts Manager
Company: PI Worldwide
Address: 16 Laurel Ave.
City: Wellesley, MA 02481
Phone: 781-235-8872
E-mail: mbcotter@piworldwide.com

5. TRAINING AND AWARENESS

The Company will provide initial and periodic training and communications to everyone with access to Client Data on security issues to make them aware of reasonably foreseeable security threats and the measures the Company has adopted to combat these threats. The Company will communicate its information security policies to employees, consultants and service providers who may have access to Client Data. Everyone must take reasonable steps to become familiar with the Company's information security policies and procedures, attend training and review information security communications.

All employees and contractors are subject to confidentiality agreements and are trained in requirements to keep Client Data in confidence as highly secure company confidential data. In addition, all employees and contractors are required to acknowledge the Company Privacy Policy.

6. EMPLOYEE ACCESS CONTROL

Access to Client Data will be granted to employees and contractors only on a "need to know" basis. Generally, only a limited group of people will have access to Client Data, including management, employees involved in consulting and technical support and the Company's web development contractor.

Access to Company systems is subject to an authorization process controlled by the Director of Information Services. Individuals are authorized for access to systems based on approval by the Director of Information Services at PI Worldwide. All employees are issued a unique user ID and are not permitted to share user ID's. All user ID's and passwords are kept confidential and are not accessible to anyone other than the individual to whom they are issued. Systems are configured so that access is denied after a certain number of unsuccessful logins.

Access to systems is terminated immediately if any employee ceases employment. All employees, consultants and service providers must return and, upon request, destroy all Client Data provided by the Company before their departure or earlier, upon the Company's request.

7. GENERAL TECHNICAL DATA SECURITY STANDARDS

The Company, through the Data Security Committee, will use reasonable efforts to monitor currently available and cost effective technical security measures so that that the Company implements and maintains a commercially reasonable level of technical data security that secures Client Data to at least the level of the Company's competitors and peers of similar market size. Currently, the Company has adopted the following general security standards for the system environment on which Client Data is housed:

System Environment Technical Controls

- System is hosted by AT&T in a SAS 70 certified facility
- All Servers (3 web servers and 2 database servers) located behind a firewall;
- All Servers located behind a network based intrusion protection device;

- All Servers are protected by an enhanced level of virus and intrusion software;
- Within AT&T System Environment, PI Worldwide has redundant and additional security as follows:
 - Access to data within database is password protected with limited access to key personnel only;
 - Access to web servers is password protected with limited access to key personnel only. There are two levels of password and authorization checking, where the systems will prevent access after multiple invalid attempts, and passwords are reset on a regular basis; and
 - Access to PI Worldwide's environment is restricted to its secured network and all access is logged and core system data is encrypted.

System Environment Physical and Environmental Controls

- AT&T hosting facility is under armed guard 24-7-365
- Only 2 AT&T employees per shift have access to the physical cage housing the machines;
- Entry can only be gained through identification, finger print and weight measurement;
- The Cage containing PI Worldwide machines are unmarked and indistinguishable from all other cages;
- The Cage is locked with keys available only within the facility with special verification;
- The facility that houses the equipment is completely fire resistant, down to special sensors that identify a fire source and automatically shut down electricity and delivers fire suppression;
- Entire facility is on an elevated floor with 2 feet of space underneath for water storage;
- The facility is backed up by on-site generators that have enough in stock fuel for 1 month of operation for the entire facility; and
- The facility is tightly air conditioned to keep air temperature and quality at optimal levels.

System Interconnection/Information Sharing

- The Servers described above are connected through a firewall and are able to transfer information back and forth within the network; and
- Data from the internal network at PI Worldwide and its development contractors are connected through a secure LAN-to-LAN connection; the only way data from the systems is transferred to the AT&T hosted environment above. As described above, all data transferred through this tunnel is secure and encrypted.

System Monitoring and Review

- Ongoing monitors watch all systems for changes in basic functionality;
- Intrusion Protection Systems monitor all traffic throughout every day for patterns;
- Each system is monitored daily by 24 hour staff. All systems have automated alarms programmed in to ensure any abnormal or problem event is tracked, logged and all staff are notified;
- Each month, tests and system upgrades are performed on all systems; and
- Passwords are changed on a regular basis or sooner based on need.

Contingency Planning

- AT&T has 10 other Tier 1 facilities in the world where Company equipment could be

- reestablished with 48 hours in case of an entire facility catastrophe;
- AT&T is providing the equipment for all services, and has immediate replacements ready if there is any failure experienced;
 - Backups are performed every hour, and moved off machine and then off-site every 4 hours at a minimum;
 - Backup facilities are available to all AT&T facilities worldwide, so a full restore of the complete site and all data is available anywhere we need to move; and
 - Backups are confirmed daily and tested every quarter.

Hardware and System Software Maintenance Controls

- Maintenance is performed every month, with a low activity window made available for all upgrades and checks to operating system upgrades;
- Intrusion Protection and Virus Protection application are updated automatically and on demand;
- All Systems and Applications are monitored continuously to check for evidence of tampering, or problems. Monitors are keyed to notify 24-7-365 on-duty personnel of any problem so corrective actions can be taken immediately; and
- All systems are periodically checked by an outside auditing firm.

8. SERVICE PROVIDERS

It is important that Client Data be kept in a safe, secure, and confidential manner whenever the Company provides it to third-party service providers, vendors, contractors, and consultants (“service providers”). Access to Client Data may only be provided to authorized service providers under written agreements that require the service provider to observe strict confidentiality obligations. To the extent practicable, the Company will require service providers who may have access to Client Data to agree by written contract to implement and maintain reasonable security measures for Client Data consistent with this Policy. All service provider contracts must be reviewed and approved by the Chief Financial Officer. The Committee shall periodically review the performance of service providers who have access to Client Data to ensure that the service providers have put in place and maintained adequate security measures.

9. MONITORING OF THIS POLICY

The Committee shall work in conjunction with all areas, departments, offices and staff to ensure that the Company’s environment continues to be secure and confidential. The Committee shall regularly monitor compliance with this Policy by the Company, its employees, consultants and service providers. The Committee shall also evaluate material changes in circumstances or business operations that require revisions to this Policy. A comprehensive review of the Policy will occur whenever there is a material change in the Company’s business practices that reasonably implicates the security or integrity of Client Data.