Information Protection

Privacy, Security, and Confidentiality Policy

Introduction

General Information

InsynQ, LLC's security policies have been developed to provide a maximum level of surety to our clients and partners that proprietary, confidential information will be kept secure and confidential.

Objectives

The policies outlined in this document allow InsynQ, LLC personnel and technologies to provide certain services and functionality to our subscribers while retaining maximum confidentiality of identity and security of customer data.

Baseline Procedures

Minimum data security and protection services provide for continuous file system scanning for virus signatures or activity, as well as on-demand and on-access scanning of certain servers and network resources. Compromised files are quarantined in secure systems, where cleaning or removal of the virus code takes place. Strict controls are placed on the quarantine systems preventing their interaction with "live" file systems on the network.

Minimum data security and protection services further provide for regular, nightly backups of data to near-line storage. Additionally, data is regularly rotated to off-line secure storage which is then periodically rotated to offsite secure facilities, ensuring protection of the archive data sets separate from the datacenter or online facilities. Typical available restore window opportunity extends for four (4) business days from date of archive. All system configurations are originally mastered (golden copy), and stored in safe vaults.

Responsible Organizational Structure

Corporate Information Services

Internal corporate information services include all systems relating to the management and operation of the InsynQ, LLC organization and technology services. InsynQ, LLC provides top-level organization, structure and management of all business units within the InsynQ, LLC organization. This includes all operational, support, and financial systems.

Business Unit Information Services

Business unit information services include all sales and marketing systems relating to the specific business units. Further, certain customer and service data is contained within business unit-specific information systems for the purposes of providing customer support and technical assistance.

Internal Organizations

The subdivision of the operating units of InsynQ, LLC into internal organizations facilitates the retention and confidentiality of certain information and data required to deliver services. Care is taken to ensure that data sinks in each operating unit are separate and secure, with limited communication or dissemination of that data to other units within the company, and only when and to the degree required to deliver services or support.

Tenants

The InsynQ, LLC organization is comprised of several tenant units:

Corporate Administration and Finance

Operations and Technology

Subscriber Support

Sales and Marketing

Security Standards

Confidentiality

Confidentiality of subscriber identity, as well as captured business and user relationship data, is kept secure and made available only to those whose responsibilities require knowledge of such data, such as customer support personnel. Specifics on subscriber identity are not required by the technical or operating units, except as it pertains to establishing permissions or file system relationships for related subscriber accounts and resources.

Integrity

The integrity of stored system information (separate from customer data) is protected through internal management processes and cross-references (validations) from production and support data sources.

Authorization

Access to certain stored system information or customer data is provided only to those authorized for an approved business process requiring access to such information. Authorization is granted only when the approved process meets technical and operational guidelines and is proven to require access to such information. Authorization to access information is not provided in blanket form, but rather is provided to allow for the minimum access required to perform the required function or facilitate the required process. Authorizations and credentials are kept strictly confidential, with access and distribution being controlled by the management of the authorizing tenant unit.

Access

Access to technical resources and facilities, information systems, or customer data is provided exclusively to those whose responsibilities require such access. All systems are protected with secure authentication to the network and individual systems required. All physical facilities are secured from public intrusion or traffic, and all server and network facilities are secured from unauthorized access by either individual or device, by datacenter facility personnel.

Acceptable Use

InsynQ, LLC employees and contractors are bound by policies for appropriate use of information and resources that might be provided in order to facilitate a specific job responsibility, function or process. Terms of InsynQ, LLC public *acceptable use* policy may be found later in this document.

Comprehensive Outline of Documented Security Policies

1. Domain Services
    a. Authentication
    b. Password Standards
    c. Resident Personnel Departure
        i. Friendly Terms
        ii. Unfriendly Terms
2. Physical Access
3. Backups
4. Retention Policy
5. Auditing
6. E-Mail Systems
    a. Authentication
    b. Intrusion Protection
    c. Physical Access
    d. Backups
    e. Retention Policy
    f. Auditing
7. Web Servers
    a. Internal
    b. External
8. Datacenter
    a. Intrusion Protection
    b. Physical Access
    c. Backups
    d. Retention Policy
    e. Auditing
    f. Disaster Recovery
9. LAN/WAN
    a. Authentication
    b. Intrusion Protection
    c. Content Filtering
    d. Auditing
    e. Disaster Recovery
        i. NOC (Network Operations Center)
    f. Physical Network Layer
10. Desktop Systems
    a. Authentication
    b. Intrusion Protection
    c. Physical Access
    d. Backups
    e. Auditing
    f. Disaster Recovery
11. Telecommunications Systems
    a. Authentication
    b. Intrusion Protection
    c. Physical Access
    d. Auditing
    e. Backups
    f. Retention Policy
    g. Disaster Recovery
12. Strategic and Legacy Systems
    a. Authentication
    b. Intrusion Protection
    c. Physical Access
    d. Auditing
    e. Backups
    f. Retention Policy
    g. Disaster Recovery
13. Security Services & Procedures
    a. Auditing
    b. Monitoring
    c. Alerts
14. Security Incident Procedures
    a. Preparing & planning for incident handling
    b. Notifications and Points of Contact
    c. Identifying an Incident
    d. Handling an Incident
    e. Forensics and Legal Implications
    f. Public Relations Contacts
    g. Key Steps
        i. Containment
        ii. Eradication
        iii. Recovery
        iv. Follow-Up
        v. Post-mortem
    h. Responsibilities
15. Ongoing Activities
    a. Incident Warnings
        i. Virus Warnings
        ii. Intrusion Vulnerabilities
        iii. Security Patches and Fixes
16. Contacts, Mailing Lists & Other Resources

SSAE 16 SOC I Type I

On February 28, 2014, Assure Professional completed and “Independent Service Auditor’s Report on Management’s Description of a Service Organization’s System and the Suitability of the Design of Controls” or an SSAE 16 Type I Audit, which covered and certified InsynQ, LLC’s controls.

SSAE 16 is generally applicable when an independent auditor ("user auditor") is planning the financial statement audit of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that impact a user organization's system of internal controls could be application service providers, bank trust departments, claims processing centers, datacenters, third party administrators, or other data processing service bureaus.

In the audit the auditor obtained an understanding of the InsynQ, LLC’s internal control sufficient to plan the audit as required. As InsynQ, LLC provides transaction processing, data hosting, IT infrastructure or other data processing services to the user organization, the auditor needed to gain an understanding of the controls at the service organization in order to properly plan the audit and evaluate control risk. The Audit showed compliance and controls applied properly in all areas.

Because InsynQ, LLC controls and operates all servers within our hosting infrastructure, the relevance of SSAE 16 to the physical facility is limited. The physical datacenter facilities and associated operators have no direct access to information or data stored within InsynQ, LLC’s application hosting infrastructure. These controls fall under the individual datacenters’ responsibility, and we require that each have at least an SSAE SOC II Type II certification.

PCI DSS

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security, and was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa LLC International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

- **Build and Maintain a Secure Network**
  - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
  - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
  - *Requirement 3:* Protect stored cardholder data
  - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  - *Requirement 5:* Use and regularly update anti-virus software
  - *Requirement 6:* Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**
  - *Requirement 7:* Restrict access to cardholder data by business need-to-know
  - *Requirement 8:* Assign a unique ID to each person with computer access
  - *Requirement 9:* Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  - *Requirement 10:* Track and monitor all access to network resources and cardholder data
  - *Requirement 11:* Regularly test security systems and processes
- **Maintain an Information Security Policy**
  - *Requirement 12:* Maintain a policy that addresses information security

Accreditation and Certification

Due to the nature of the applications and associated data hosted on behalf of our customers, InsynQ, LLC has been a key participant in SSAE 16, PCI DSS, and other auditing processes and certification procedures throughout our service history. In most cases, these audits were performed as part of a larger auditing and validation process involving the subscribing customer organization, either public or private, and where the audit reports and certifications are held in the name of the customer.

One of the key elements of SSAE 16 and other relevant accreditation processes is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers in a uniform reporting format. The review and issuance of certification of these processes as performed by the MSPA (Managed Service Provider Alliance), key independent software companies, and technically-oriented industry associations signifies that InsynQ, LLC's service organization has had its control objectives and control activities examined by independent accreditation organizations.

In addition to SSAE 16 compliance, PCI DSS compliance, tax data processing and e-file transmission approval, and other relevant certifications and approvals in which InsynQ, LLC has been a participant, InsynQ, LLC's service have been reviewed, audited, or accredited by the following independent organizations:

- MSPA: Independent Managed Service Provider Accreditation
- ITA: Information Technology Alliance Accredited Member
- Sage Software: Certified Hosting Provider
- Intuit, LLC: Licensed Hosting Provider
- Microsoft: SPLA Licensor and Hosting Provider
- Authorize.Net: PCI DSS Approval

Acceptable Use Policy

This document defines the Acceptable Use Policy ("Policy") of products and services provided by InsynQ, LLC, LLC to all of its clients and other users (collectively, "Client"). This Policy will ensure the integrity, security, reliability, and privacy of the InsynQ, LLC network, systems, products, services, server hosting facilities and data contained within (collectively, the "InsynQ, LLC Network"). InsynQ, LLC retains the right to modify the Policy at any time, effective upon posting of the modified Policy to InsynQ, LLC's corporate website. Client is responsible for continual compliance of this Policy as well as any modifications thereto posted.

InsynQ, LLC Network Security

Client is prohibited from violating, or attempting to violate, the security of the InsynQ, LLC Network. Any violations may result in criminal and civil liabilities to the Client. InsynQ, LLC will investigate any alleged violations and will cooperate with law enforcement agencies if a criminal violation is suspected. Examples of violations of the security of the InsynQ, LLC Network include, without limitation, the following:

- Accessing data not intended for such Client
- Logging into a server or account which the Client is not authorized to access
- Breaching security or authentication measures without proper authorization
- Attempting to interfere with service to any user, host, or network including, without limitation, via means of overloading, “denial of service,” "flooding," "mail bombing," "spamming" or "crashing"
- Taking any action in order to obtain services to which the Client is not entitle

Illegal Use

The InsynQ, LLC Network may only be used for lawful purposes. For example, Client may not use the InsynQ, LLC Network to create, transmit, distribute, or store material that:

- Violates a trademark, copyright, trade secret, or other intellectual property rights of others
- Violates the privacy, publicity, or other personal rights of others
- Impairs the privacy of communications
- Contains obscene or pornographic content
- May be threatening, abusive, or hateful
- Violates export control laws or regulations
- Encourages conduct that would constitute a criminal offense or give rise to civil liability
- Causes technical disturbances to the InsynQ, LLC Network, including, but not limited to, introduction of viruses, worms, or other destructive mechanisms
- Violates reasonable regulations of InsynQ, LLC or other service providers with respect to the network
- Assists or permits any persons in engaging in any of the activities described above
- Constitutes deceptive on-line marketing

If Client becomes aware of any such activities, Client is obligated to immediately notify InsynQ, LLC and take all other appropriate actions to cause such activities to cease.

Unsolicited Communications

Posting the same or similar unsolicited e-mail messages, bulk commercial advertising, or informal announcements to one or more groups (known as "Spam") are prohibited. Spam is not only annoying to Internet users; it seriously affects the efficiency and cost-effectiveness of the InsynQ, LLC Network. These unsolicited messages can increase your costs by clogging the InsynQ, LLC Network, rendering your website inaccessible and potentially leading to down time of your mission-critical applications.

In addition, both User Group and e-mail users may not:

- Send or post e-mail messages which are excessive and/or intended to harass or annoy others
- Continue to send e-mail to a recipient that has indicated that he/she does not wish to receive it
- Send e-mail with forged TCP/IP packet header information
- Intentionally omit, delete, forge, or misrepresent transmission information, including headers, return addresses, information
- Take any other actions intended to cloak the Client's identity or contact information

Content

Client is responsible for all its content hosted by InsynQ, LLC. InsynQ, LLC exercises no control over, and accepts no responsibility for, the content of the information passing through the InsynQ, LLC Network, including content provided on any third party websites linked to the InsynQ, LLC Network. Any website links are provided as Internet navigation tools for informational purposes only and not as an endorsement by InsynQ, LLC of the contents of such websites. InsynQ, LLC does not adopt, nor warrant the accuracy of, the content of any linked website and undertakes no responsibility to update the content. Use of any information obtained via the InsynQ, LLC Network is at Client's own risk.

InsynQ, LLC does not screen communications and is not responsible for screening or monitoring content used by Client.

Consequences of Unacceptable Use

InsynQ, LLC reserves the right to suspend or terminate access to the InsynQ, LLC Network upon notice of a violation of this Policy.

Indirect or attempted violations of this Policy, and actual or attempted violations by a third party on behalf of a Client, shall be considered violations of this Policy by such Client. Furthermore, it is a violation of this Acceptable Use Policy to use the services of another provider for the purposes of facilitating any of the activities described above if such use of another provider's service could reasonably be expected to affect the InsynQ, LLC Network.

Questions, Comments, or Concerns

InsynQ, LLC reserves the right to modify this Policy in the manner set forth above at any time. If you are unsure whether any contemplated use is permitted or have any comments regarding prohibited use or other abuse of the InsynQ, LLC Network, please direct questions or comments to InsynQ's support line: 253-857-9400.

Privacy Policy – General

InsynQ, LLC has created this privacy statement in order to demonstrate our firm commitment to privacy. The following discloses the information gathering and dissemination practices for the InsynQ, LLC corporate website.

Information Automatically Logged
We use your IP address to help diagnose problems with our server and to administer our website. Your IP address is also used to help identify you when you order services, and to gather general subscriber demographic information.

Registration Forms

Our site's registration form requires users to give us contact information (such as name, email, and postal address), service information, and demographic information. Certain financial information (such as bank account or credit card numbers) are **not** requested on unsecured forms.

Contact information from the registration forms is used to create service, and to provide information about our company. The customer's contact information is also used to get in touch with the customer when necessary, and will not be shared with other companies who may want to contact our customers for other purposes.

Financial information that is collected is used to bill the user for products and services, and to assist with the collection of service fees.

Surveys

Our online surveys may ask visitors for contact information (such as email address). Contact information from the surveys is used to qualify the nature of the survey results.

Information Collection and Use

InsynQ, LLC has created this privacy statement in order to demonstrate our firm commitment to privacy. The following discloses our information gathering and dissemination practices at InsynQ, LLC.

InsynQ, LLC will not sell or rent the personally identifiable information of its customers.

Our product uses a registration form for customers to activate their service. We collect customer contact information (such as their e-mail addresses) and financial information (such as their credit card numbers). Financial information that is collected is used to bill the customer for products and services. Contact information from the registration form is used to send the customer information about our company, inform the customer they have enrolled in services, and/or we need to update the customer on the service. InsynQ, LLC maintains the right to email/contact the customer for the purpose of administering our services. In addition to the services InsynQ, LLC provides, we may run surveys and promotions on our site and ask visitors for contact information (such as their e-mail address). We use contact data to send users information about our company.

InsynQ, LLC's websites may contain links to other sites. InsynQ, LLC is not responsible for the privacy practices or the content of such websites. We encourage our users to be aware when they leave our site and to read the privacy statements of every website that collects personally identifiable information. This privacy statement applies solely to information collected by InsynQ, LLC. InsynQ, LLC may disclose personal information when required by law or in the good-faith belief that such action is necessary in order to conform to the edicts of law or comply with a legal process served on our website. The usage of cookies is in no way linked to any personally identifiable information by InsynQ, LLC. Some of our services use cookies to help optimize the performance of the web features on our software. Our software will function with or without the use of cookies.

Sharing

We may share aggregate demographic information with our partners. This sharing is statistical and does not disclose any personal information that can identify any individual person. We may use a credit card processing company to bill users for goods and services. We may partner with other parties to provide specific services. When a customer places an order or signs up for these services, names or other contact information that is necessary to provide these services may be shared between the parties. These parties are not allowed to use personally identifiable information except for the purpose of providing their specific service(s).

Notification of Changes

If any material changes are to be made in our privacy practices we will, 30 days prior to the changes taking effect, send a notification to the email address provided by the customer and post the changes in our privacy statement on our homepage.

Security

InsynQ, LLC has security measures in place to protect the access, loss, misuse and alteration of the data and personally identifiable information under its control. The security and integrity of customer data is our business. At InsynQ, LLC access to customer's personally identifiable information is limited to e-mail addresses, contact and billing information. Credit card information is kept solely within InsynQ, LLC's billing system.

Correct/Update

We provide users the following options for changing and modifying information previously provided.

1. Contact billing@insynq.com
2. Submit change using account management system SSIT

Physical Security and Datacenter Access

Only previously approved individuals may access InsynQ, LLC's data center and co-location facilities. Access is limited to designated areas for the placement or servicing of InsynQ, LLC equipment.