IT Security Policy

Version	Date	Issued By
V.3	20/02/2024	S.Sahota

Intouch Internal IT Systems

System Breach Protocol

In the event of a system breach we would immediately terminate access to the breached account. All employees would be emailled within 30 mintues and asked to change their passwords. In addition, we would launch an investigation into the breach within 1 working day.

Employee leaving Protocol

In the event of an employee leaving we would immediately terminate access to their company account(s). Any passwords known to that employee would be changed.

Access Control Lists

All devices within Intouch Monitoring Ltd company control employ some form of Access Control List (ACL) including but not limited to servers, firewalls and web servers.

Port Blocking

All ports are blocked, with the exception of 443, 143, and 25.

Network Monitoring Facility

The network is monitored by an SNMP monitoring agent.

Intrusion Detection Systems (IDS)

Intouch Monitoring Ltd company has Bit Defender Firewall enabled and virus protection, with Barracuda Web protection, which is used for threat logging and email alerting.

Internal Employee Password Policy

• Employees must report any suspected security breach immediately to the IT system administrator as soon as the issue is identified.

• All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least eight characters long. These requirements will be enforced with software when possible.

• In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective. These requirements will be enforced with software when possible.

• A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. These requirements will be enforced with software when possible.

• Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.

• Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

• Employees will be required to register for multi-factor authentication and must register contact information such as email address, phone number etc. Employees must keep these contact details up-to-date so they can respond to security challenges and be notified of security events.

• Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

• Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

• Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognize these attacks.

• Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

• Employees may not use password managers or other tools to help store and remember passwords without permission.

Anti-Virus System
For Internal company spam, malware & virus protection Intouch uses Bit Defender. For internal company email and web protection Intouch uses Barracuda. All employees are required to undergo the National Cyber Security Centre IT security awareness e-learning training course.

Physical Security
The Intouch premises are always manned during office hours and locked out of office hours and monitored by CCTV. The industrial site where our premises is located is protected out of hours by pin code accessed gates.

i4Cloud Application Security

External Customer Password Policy

i4 Cloud enforces a minimum password complexity. System administrator (external customer) can set a password expiration period.

Event Logging

All actions are recorded within the system and reportable. The event logs in the system cannot be deleted or modified. A record is kept of all 'log on' events, including failed log on attempts.

i4 Cloud domains

All i4Cloud domains are secured with an SSL certificate.

Data Separation

Intouch does not comingle customer data (each client has its own database(s)).

Data Destruction

Inherited Microsoft's from Azure. Any data held about customers outside of Azure (accounts etc.) is kept in accordance with UK tax requirements, and then securely disposed of.

Controls

i4 Cloud is hosted on Microsoft Azure.

Redundancy

Data is stored in a Microsoft Azure SQL Database Managed Instance and is protected with automated backups.

Disaster Recovery and Backups

Microsoft Azure SQL Database Managed Instance data is protected with automated backups.

High Availability

Microsoft Azure SQL Database Managed Instances SLA is 99.99% availability