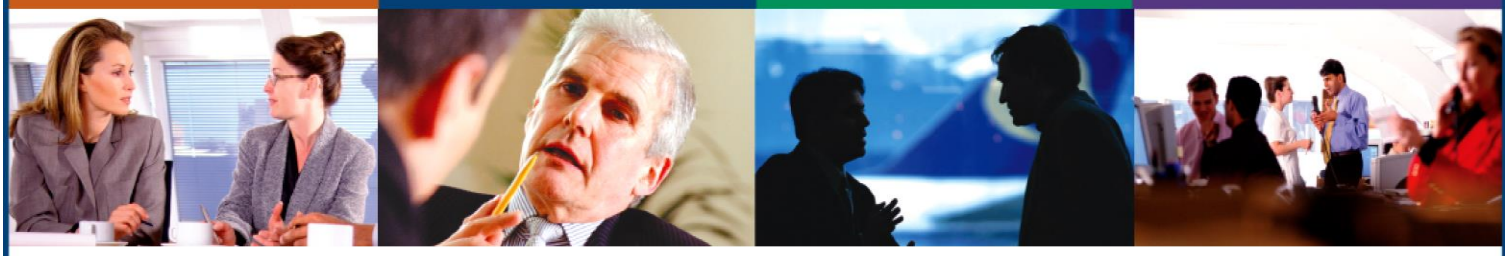

Sales for the *mobile* professional

JANUARY 1, 2017

SalesNOW

Security Policy – v.1.7 2017-01-01

Overview

Interchange Solutions Inc. (Interchange) is the proud maker of SalesNOW®. Interchange understands that your trust in us depends on how well we keep your personal, business, and account information secure. Interchange utilizes some of the most advanced technology for Internet security available today. When you access the SalesNOW® site using industry standard Secure Socket Layer (SSL) technology, your information is protected using both server authentication and data encryption ensuring that your data is available to only registered users in your organization. In addition, www.salesnow.com is hosted in a secure server environment that uses a firewall and other advanced technology to prevent access from outside intruders. This document outlines some of the mechanisms and processes that we have implemented to help ensure that your data is protected, including:

1. Secure Transmission and Sessions
2. Network Protection
3. Secure Data Centers
4. Backups and Disaster Recovery

Secure Transmission and Sessions

1. Data Encryption

Credentials and data being synchronized are encrypted by SSL certificates issued by Symantec Corporation which is the largest SSL issuer in the world. The communication between your computer or mobile device and our servers is encrypted using 128-bit keys (256-bit keys in many cases). What this means is that even if the information travelling between your computer or mobile device and our servers were to be intercepted, it would nearly be impossible for anyone to make any sense of it. The SSL Security level can be configured by the administrator as follows:

- SSL is enforced during the login on the web browser
- SSL is optional for any other forms of data access, such that data is protected by SSL for over the air transmission.

2. Cookies

We use cookies as an additional security feature. There are two common types of cookies that we use, "session cookies" and "persistent cookies". Session cookies store information only for the length of time that you are connected to our website - they are not written onto your hard drive. Once you leave the website, the originator of the cookie no longer has the information that was contained on it. Throughout your session, the session cookie acts as a type of digital signature to identify your current session to the Web Server.

The information stored in "persistent cookies" is written onto your hard drive and remains there until the expiry date of the cookie. Interchange uses persistent cookies to store non-sensitive information that you are aware of and have agreed to. For example, if you choose the option on our login screen to remember your login Email, the system will remember and automatically input your logon Email each time you access SalesNOW®.

3. Username and Password

Each SalesNOW® user will be assigned a unique user name which is associated to their email address. New users who provide us with their email address are required to verify themselves by clicking on an activation email. During the activation process, new users are prompted to create a unique password. This password can and should be modified by the user on a regular basis. The user must enter their unique Email and password combination to gain access to the SalesNOW® system, either from the Web or on your Android®, BlackBerry®, iPhone® or iPad® device. All log-ins are tracked on the SalesNOW® server and the log-in history is kept for 90 days. The account, IP, browser information and/or device information are also tracked. Individual user sessions are identified and re-verified with each transaction, using a unique token created at login.

Network Protection

1. Secure Firewalls

SalesNOW® is hosted in secure hosting environments that use secure firewalls and up to date security technology to prevent unauthorized access to our internal systems. All computers in our hosting environments are monitored on a consistent basis to ensure that your data is kept safe from viruses, hackers, and competitors.

We have Internet firewalls designed to securely separate the Internet from our internal computer systems and databases. Data coming from customer computers via the Internet flows through a series of safety check points on its way to our internal systems so that only authorized messages and transactions enter our computer systems.

2. Virus Scanning

All computers in our hosting environments are monitored on a consistent basis to ensure that your data is kept safe from viruses, hackers, and competitors. Traffic coming into SalesNOW servers is automatically scanned for harmful viruses using state of the art virus scanning protocols which are updated on a regular basis.

3. Intrusion Detection and Protection

In Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts and reports. SalesNOW has deployed a Relentless Intrusion Detection (RID) system which employs cloud-powered technology to identify automatically behaviour patterns that are missed by most traditional stand-alone network security products, with possible threats subjected to round-the-clock expert analysis.

It integrates with our SalesNOW infrastructure to block potentially malicious activity, stopping attacks such as unauthorized log in attempts and remote command execution. If human attackers, network worms or bots are at work, SalesNOW is instantly alerted so that we can respond quickly and block them before they threaten your entire network.

This RID system not only provides defense against immediate threats – it regularly scans internal and external networks, to determine if there are any vulnerabilities in SalesNOW. And real-time systems and processes are tested quarterly to maintain the highest level of security compliance.

Secure Data Centers

1. Physical Security

Closed circuit televisions and 24x7x365 onsite security teams vigilantly protect our datacenters. Military-grade pass card access and biometric finger scan units provide even further security.

2. Environmental Controls

Our servers will always be kept at the optimal temperature for performance. Our heating ventilation air conditioning (HVAC) systems have full particle filtering and humidity control. The climate within each of our datacenters is maintained according to ASHRAE Guidelines.

3. Uninterrupted Power

Our on-site, diesel-powered generators and uninterruptible power systems (UPS) deliver redundant power if a critical incident occurs. We regularly test our infrastructure to perform as designed in the event of an emergency. And we back it all up with our 100% Power SLA and 100% Network Uptime SLA.

4. NOC Support

While the majority of datacenter sites are network neutral, we have our own on-site NOC (Network Operations Center), managing 13,000 route miles of fiber around the world. This network is supported by engineers and Level III system administrators that deliver support 24x7x365.

5. Fire Detection and Suppression

Sprinkler systems are installed with double interlock pre-action and detection system functionality. The systems are designed in such a manner that water does not enter the sprinkler system piping during normal operations. Pre-action detection and intelligent heat detectors are installed in the ceiling of mission critical areas.

Backup and Disaster Recovery

1. Real Time and Daily Backup

On mobile devices, data is only stored within the dedicated application store to ensure security. On servers, the information is being stored in a Password Protected Secure LAN Server. Servers are all monitored by an automated service so IT associates are notified upon system failure. Servers are clustered and data is regularly backed-up. This allows the inactive nodes of the clustered servers to take

on the role of the disabled servers. If the database servers encounter catastrophic errors, data can always be restored from the full data backup and transaction logs. Even if a user deletes data, that data can be restored from within the users' account. Our support team can also recover any data that your users may delete. When setting up your users you can determine who has the ability to delete records.

2. Redundant Power

In addition to the use of uninterruptible power supplies and diesel engine generators, our data centers have two independent utility sources in place, originating from independent feeders or substations.

3. Redundant Internet

SalesNOW is connected to the world and to you through multiple Tier 1 ISPs. So if any one ISP fails or experiences delays, SalesNOW can automatically utilize another ISP so that you can still reliably get to your data and application.

4. GEO Mirroring

Customer data is mirrored in separate geographic locations for Disaster Recovery and Business Continuity purposes.

Security is Everyone's Responsibility

At Interchange, we take the safeguarding of your information seriously. In fact, we believe keeping information about you safe and secure is every employee's responsibility. All employees of Interchange are aware of the procedures that must be taken to safeguard customer information. It is specified in our employment agreements and regularly confirmed in writing. We also encourage you, the customer, to take steps in protecting information about you.

Here is How You Can Help

While we at Interchange continue to provide security controls to protect information about you, we believe it is extremely important for you to share in the responsibility for security. The following are some ways you can protect yourself and your accounts:

- Never share your password with anyone.

- We recommend you change your password on a regular basis. If you think your password has been compromised, change it immediately.
- Consider using a personal firewall to prevent hackers from invading your personal computer, especially if you are using DSL or a cable modem to access the Internet.
- Install virus protection software and scan all downloaded software before use. Also, delete emails with attachments from unknown sources.
- When you are done with your transactions, always click on the Sign Out link on the website to exit the application and prevent further access to your account. When using a public PC also close the browser when you are finished.
- On your mobile device be sure to set a password with an appropriate time-out period to ensure the device is locked should you misplace your Android®, BlackBerry®, iPhone® or iPad® device.

Additional Information

SalesNOW® encourages security researchers or system administrators to report any vulnerability to secure@salesnow.com (mail to: secure@salesnow.com).