

# Security—Our Way of Doing Business

## SmartOffice Business Continuity and Disaster Recovery Plan

At the SmartOffice division of Ebix, Business Continuity and Disaster Recovery are a continuous process. Our Disaster Recovery Readiness Unit tests our strategy on a quarterly basis. Testing is completed in each environment.

We have hosted sites located in different metropolitan areas for both production and disaster recovery. We continuously validate offsite database backups for every production instance and actively synchronize production and disaster recovery instances.

Resources are located in California, Colorado, Virginia, Ontario (Canada), Nagpur and Chennai (India). Documentation and recovery tools are replicated at each site as well. Our staff is set up through a virtual private network to be able to access resources 24x7x365 from remote locations.

We constantly strive to improve the process at every opportunity. To ensure continuous readiness, we hold quarterly awareness training and quarterly Business Continuity response procedure training.

## Committed to Your Protection

At SmartOffice, protecting your critical data is an integral part of our business. From the configuration of our systems to the training of our expert staff, we build security into every aspect of our operations. The result is a total commitment to world-class security and privacy. That commitment is no empty promise: SmartOffice meets rigorous standards for information security. Our ISO 27001 certification means that we adhere to internationally recognized best practices that go beyond the guidelines set out in some other standards (such as SAS 70).

## Physical Security

SmartOffice's attention to physical security extends to its co-location facilities as well as its corporate offices. Our tier-1 co-location facilities feature 24-hour physical security, palm print and picture identification systems, keycard access, redundant electrical generators and data center air conditioners, fire suppression systems, video monitoring, and backup equipment designed to keep servers continually up and running. Our corporate offices have well-defined security zones enforced by keycard systems that restrict access to sensitive areas to authorized personnel.

## Application Security

SmartOffice recognizes that your data belongs to you and must be protected from access by other customers. We require a valid office name, user name, and password to access our systems (all of which are encrypted during transmission, as described in Network Security). Also, our robust application security model is reapplied with every data request and is enforced for the duration of a user session. SmartOffice also enforces tight security at the operating system level. We use a minimal number of access points to production servers, protect accounts with strong passwords, and disable and/or remove unnecessary users, protocols, and processes. Operating systems are maintained at each vendor's recommended patch levels for security.

## Data Security

To ensure the integrity and safety of your data, we maintain a top-tier storage and backup system. Customer data is stored on carrier-class EMC storage systems for ultimate reliability, using RAID disks with multiple data paths. In addition, SmartOffice follows a meticulous backup regimen. Your data is backed up several times during business hours onto easily retrievable near-line storage. Those backups are stored on a redundant Storage Area Network (SAN). We also capture a daily snapshot of your data that we send to a remote data center using a highly secure connection (see Network Security for details).

Finally, all of our systems follow strict Trusted Computing Base guidelines to ensure that the components necessary for optimal security are in place and functioning properly.

## Network Security

SmartOffice's network offers the highest possible protection using multiple security layers and industry-leading hardware and software solutions. Our network perimeter is protected by multiple Cisco PIX firewalls. Inside those firewalls, SmartOffice systems are safeguarded by network address translation, port redirection, IP masquerading, non-routable IP addressing schemes, and other methods. In addition, SmartOffice has a comprehensive intrusion detection system to guard against network and host attacks. Our security team monitors and analyzes firewall logs and takes quick action when security threats are identified. Industry-leading tools such as Snort, OSSEC, Aانval, and McAfee form the basis of the system, which features frequent intrusion and malware signature updates to ensure the most current level of protection possible.

We also make every effort to ensure that data transmitted over the Internet, both by us and our customers, is secure. We use virtual private network (VPN) technology (3DES-encrypted IPsec tunneling) to transfer data between data centers and to remotely administer servers, with RSA SecurID two-factor authentication tokens required for VPN access.

Traffic between your Web browser and our systems is encrypted with 128-bit VeriSign SSL Certificates and 1024-bit RSA public keys; the lock icon in your browser is your assurance that the information you send and receive over the Web enjoys the highest level of protection available.

## Operations Security

The day-to-day management of our hosted systems includes important procedures for maintaining security in our overall system. One way we ensure operations security is by using a clear, logical procedure when making changes to our infrastructure, operations, security, and other important operational areas. The procedure involves proper authorization, development, deployment, and review of changes to ensure that they are done properly and will not adversely affect our customers' use of the system. Our system of internal audits also helps to ensure that SmartOffice complies with certification requirements.

Employee training is also critical. Only a limited number of "classified employees" are allowed to access systems containing customer data to perform maintenance, monitoring, and backups. Classified employees undergo background checks, regular security training, and random audits of their work. Furthermore, all SmartOffice employees are trained periodically on proper procedures for securing computers and other sensitive information and guarding against viruses and related threats that could compromise company and customer data.

## Reliability

System outages cost time and money, which is why we take steps to make reliability a hallmark of our service and to minimize downtime. Our network switches and firewalls are configured redundantly to prevent a single point of failure from bringing down the entire system. In addition, SmartOffice has a comprehensive Business Continuity Plan for managing unexpected disruptions ranging from power and equipment failures to environmental disasters and criminal acts. SmartOffice has multiple data centers in different cities across the United States and Canada that can be brought online quickly in the unlikely event that our production facilities are rendered unavailable. We review and test our disaster recovery plan quarterly.

## Ongoing Review and Improvement

SmartOffice constantly monitors, reviews, and improves security controls, policies, and procedures to maintain its certification and ensure the best possible protection for customer data. As part of that process, we run monthly internal vulnerability threat assessments against all hosted systems. SmartOffice also contracts with a third party to perform annual penetration tests and quarterly vulnerability threat assessments against all of our web-facing systems and, all aimed at uncovering vulnerabilities and errors that need to be addressed. Combined with our internal security audits, these procedures help strengthen our commitment to your security. With SmartOffice hosting solutions, you can run your business with the utmost confidence.

