SmartOffice

Security-Our Way of Doing Business

Committed to your Protection

At Ebix, 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.

SmartOffice Business Continuity and Disaster Recovery Plan

System outages cost time and money, which is why we take steps to make reliability a hallmark of our service and to minimize downtime.

Hosted sites are located in different metropolitan areas for both production and disaster recovery, and recovery sites can be brought online quickly in the unlikely event that our production facilities are rendered unavailable.

Our technical experts—located in Sydney, Nagpur, and Chennai (India)—are ready to respond to crises 24x7x365.

Physical Security

Ebix's attention to security extends to its co-location facilities and corporate offices. Our tier-1 co-location facilities feature 24-hour physical security, palm print and picture identification systems, key card access, redundant electrical generators and data centre air conditioners, fire suppression systems, video monitoring, and backup equipment designed to keep servers up and running.

Application Security

SmartOffice recognizes that your data belongs to you and must be protected. We require a valid office name, user name, and Password to access our systems, and we offer multi-factor authentication for extra account protection.

In addition, 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. Server operating systems are maintained at each vendors recommended security patch levels.

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 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 and nightly 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 centre using a highly secure connection.

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 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, Ebix has a comprehensive intrusion detection system to guard against network and host attacks. Our security team monitors and analyses firewall logs and takes quick action when security threats are identified.

The system 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 our customers and us, is secure. We use virtual private network (VPN) technology with strong encryption to transfer data between data centres and to remotely administer servers, with two-factor authentication tokens required for VPN access.

Traffic between your web browser and our systems is protected with industry-standard Transport Layer Security (TLS) using 256-bit AES encryption. 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 areas. The procedure involves proper authorisation, development, deployment, and review of changes to ensure that they are done correctly and will not adversely affect our customers' use of the system.

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. 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.

Ongoing Review and Improvement

Ebix constantly monitors, reviews, and improves security controls, policies, and procedures to 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 penetration tests and 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.