infopreserve™

# Security & Reliability of PreservationVault

Keeping your data safe is our priority. From the initial design of our PreservationVault platform, we built security and reliability into the platform, engaging a third-party cyber security firm to ensure all aspects of our operations including our hardware, software, and policies and procedures meet or exceed all industry standards.

First, we go to great lengths to ensure you are the only one who can access and see your data (even our employees do not have access). Second, we build in multiple redundancies to ensure continued operation when components fail. Third, in the highly unlikely chance of a catastrophic failure, we have plans in place to ensure we quickly get you back up and running.

## Data Access Controls

- Our operations are maintained in a private data center running on our servers.
- We know EXACTLY who has access - only our employees have access to the servers.
- We do not have access to any of your data. Your data belongs to you. We have no right (or ability) to view the information. Should you elect to no longer utilize our services, you have a right to the return of all your information.
- Four levels of physical security control access to the data center including bio-metric controls.
- The datacenter is monitored 24/7 via IP video surveillance cameras.
- Our datacenter is SSAE16 Level II certified.
- All information in transit is always encrypted.
- Your biggest security risk will always be users of the system, so we have built-in configurable access controls and full audit trails to allow you to monitor and control access to your account.

## Maximizing Uptime

- Infrastructure engineered to 99.999% reliability.
- Since our launch in 2010, uptime has exceeded 99.999% outside of previously scheduled maintenance windows. In that time, we had one unscheduled outage of our servers that lasted more than a couple hours as the result of a Microsoft Windows update.
- Customers are notified of all maintenance windows, and they are scheduled for off-hours.
- All data is stored on a RAID6 storage array. This means if up to 2 hard drives fail simultaneously, no uptime is lost.
- All servers have redundant power supplies. If one fails, the server will continue to operate.
- All hardware (servers, firewall, switches, etc.) are covered under a 4-hour replacement contract.
- All security patches and upgrades are staged and deployed on a regular schedule. Upon release they are installed on our QA and development servers. If no issues are encountered for at least a week, the patches and upgrades are installed on our production servers.
- Firewalls, routers, and other network infrastructure are enterprise-grade and are designed to prevent intrusion and downtime resulting from external attacks.

- Connectivity is provided via three different service providers with each entering the building from different sides.
- N+1 redundancy of all power, network providers, fire suppression, and HVAC services.
- In addition to built-in backup redundancy, on-site backups are conducted in real-time and offsite backups are conducted weekly.

## Disaster Recovery

In the highly unlikely event that our datacenter becomes completely inoperable, InfoPreserve has a disaster recovery plan in place to restore service within 48 hours utilizing offsite backups:

- Notify customers of expected downtime.
- Utilize servers in backup datacenter (will utilize stock servers & hardware available through data center provider).
- Install & configure Windows, Microsoft SQL, and all other required applications.
- Restore database and web applications along with customer data from offsite backup.
- Reconfigure DNS to point to new servers.
- Notify customers of restoration of service.

## Monitoring Usage

Today, every reputable cloud service provider will have state-of-the-art hardware and software in place to prevent unauthorized access to your systems, so these types of breaches are extremely rare. Almost every breach today is the result of human interaction. To minimize the risk, you should not only have a plan in place, but be vigilant in making sure your employees are following the plan.

While most data breaches resulting from human interaction are not the result of willful misconduct by employees, a disgruntled employee willfully causing a breach is still a risk. To help prevent such breaches, InfoPreserve monitors and stores everything that every user does from where they logged in from to what they downloaded and viewed. First, if employees know their actions are being monitored, they are highly unlikely to purposely do something they shouldn’t. In the rare case where an employee does do something they shouldn’t, by monitoring their activity you can minimize the potential risk and damage.

## Privacy of Your Information

When you place your information in a third-party platform, determining what rights you are granting the provider is important. With many providers, you may be granting them rights to access and use your information. At InfoPreserve we take privacy seriously. Your information belongs to you, and we have no right to access that information without your permission. If you want to export your information, it belongs to you, and you have full rights to remove it. While we often assist our customers with the process of migrating their documents and records, since in this process we could potentially see the contents of some documents or records, we sign a non-disclosure agreement to protect your rights before we begin.