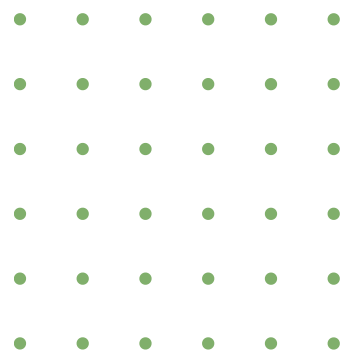




Security & Backup Overview





Table of Contents

Introduction	3
Hardware & Software	3
Backups & Disaster Recovery	3
Security	4
Updates & Testing	6
Electronic File Sharing	7
Data Retention	8



Introduction

The NewOrg Management System is a hosted, web-based solution for nonprofit data management. The NewOrg System is hosted in a secure and redundant private cloud environment expected to maintain 99.9% availability. This document explains the basic environment and the policies and procedures used to maintain availability, ensure data integrity, prevent data loss, and guard against intrusions.

Hardware & Software

The NewOrg System is hosted in a private cloud with redundant power, networks, and internet. Hosting is at secure data centers in either Dallas or Toronto.

The NewOrg platform is based on Microsoft SQL Server, Internet Information Server, VB/ASP, C#, and .NET. Each client database is separate and has its own admin user security.

Backups & Disaster Recovery

All NewOrg databases and systems are backed up nightly. Backups are both to a local storage array and sent to a second offsite location. All data is encrypted at rest and in transit.

Failover facilities are in Chicago and Vancouver.



Security

The NewOrg System has several layers of security, each overlapping. The NewOrg servers are protected by a managed enterprise-class hardware firewall that monitors the network for suspicious activity. The individual servers have secure operating system configurations and software firewalls. Database and web layers are separate, and firewalls block all ports, with admin access restricted to specific IP addresses via VPN.

Secure access to the servers is limited to our software engineering group via auditable accounts. Client access to the Application layers is provided through TLS encryption (minimum 256-bit) with login using a username and password and multi-factor authentication via SMS or email. Suspicious login attempts are monitored. IP addresses are automatically locked out after multiple failed attempts.

Perimeter Security allows NewOrg partners to restrict access to their public facing portal and Administrative login sites to specific countries or continents. User's activity is restricted through flexible permission levels set by the Client's System Administrator or NewOrg Support. All activity within the system is stored in an audit table that allows administrators to review record views, and field level update, insert or delete activity by user, date/time, field, activity type, etc.

All NewOrg forms employ SQL injection protection and public facing forms employ CAPTCHA technology. Client Data is the most important aspect of our business. NewOrg provides all of our clients with the best practices in data management/data loss/backups and disaster recovery by providing both nightly backups and encrypted offsite backups.



Both system backups (Veeam hourly snapshots) and Database Backups (nightly) are stored locally and at secondary DR sites. Backups are encrypted in transit and at rest. NewOrg maintains 30 days of daily backups to provide for data integrity and recovery issues.

All Client Data is located in a secure hosting facility in Dallas or Toronto with the following security features:

- ✓ Hardware firewall with all ports blocked except http and https
- ✓ NewOrg implements antivirus protection, hardware and software firewalls, account lockouts after failed login attempts, and optional IP restrictions by country or region on all application and database servers.
- ✓ Redundant hardware, power, and internet -Internet traffic monitoring
- ✓ TLS (Up to 512-bit encryption driven by user's browser encryption levels)
- ✓ User/password with failed attempt monitoring and auto account locking
- ✓ Provides two-factor authentication through the platform via SMS or Email Confirmation
- ✓ Overall, the NewOrg platform has been engineered to meet or exceed industry best practices for security as well as compliance with HIPAA, PIPEDA, and GDPR requirements.



Updates & Testing

NewOrg updates are tested thoroughly before being deployed. Major updates or feature changes are deployed to voluntary beta test customers for a minimum of 2 months before wider deployment.

NewOrg conducts regular audits related to security and data integrity. Below are the broad types of audits performed.

User Account Audits – check for unused or dormant user accounts on all client systems. Check for changes to user accounts or permissions. Frequency: quarterly

Firewall Rules & Logs – Constant monitoring of firewall & network activity. Frequency: daily

Account Logins – Constant/active monitoring of logins and login failures. Weekly auditing of failed login IP/Country origins. Frequency: daily/weekly

Backup Audits – Random backup checks for on-site and remote backups. Frequency: at least monthly per facility

Penetration Testing – Regular testing of core application endpoints and pages for vulnerabilities. Client-specific portal pages are tested before deployment. Frequency: quarterly



Electronic File Sharing and Signatures

NewOrg allows users to share documents and forms with clients and other external stakeholders electronically through a secure File Sharing center. Any file or document can be shared, while Print Forms and PDF files can be shared with places for Signatures or other input to be collected. Additionally, staff can request documents to be uploaded by stakeholders.

How it works

Staff can select documents, Print Forms, and Signable PDF files and share a link to them with a stakeholder via email or SMS. No files or client information is sent via email, just the link. Access to the document can be provided with a username/password (client portal) or via a secure token (random SHA1 encrypted ID) When the stakeholder follows the link to the Document Center, all data transmitted is via 256 or greater encryption. The following information is stored related to the signed document (other than any fields collected from the user in the document itself):

- NewOrg contact ID of the person signing
- Signature (URI)
- Date/Time
- IP Address of signing device
- Latitude and Longitude of device/IP
- Browser/device details

Document and Print Form details, and metadata are stored in the NewOrg Audit tables.



Data Retention

NewOrg maintains a permanent history of all data, and all access to, and changes to, data for active partners. If requested, to meet retention and disposal requirements for specific partners, NewOrg can provide an annual purge of data older than a specified age.

Purged data can be deleted completely or archived in an encrypted and offline state. Purged data will cycle out of our primary backups in 30 days

