Neighborly Software

Hosting & Security Executive Summary

- Hosted in the cloud by Microsoft Azure – no IT infrastructure required
  - All data stored in US FedRAMP certified Microsoft datacenters
  - Geo-replication across multiple U.S. data centers for business continuity
  - System accessed via web browser – no IT support required
  - Supported on all modern web browsers (i.e. Chrome, Firefox, Edge, Safari, IE v11+)
  - Additional information on Microsoft Azure security and SOC compliance assessments can be found here: https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx

- Automated data backups
  - Weekly data backups performed automatically and stored for 6 months
  - Point In Time Restore to any point within the last 35 days

- Advanced security features
  - Two factor authentication, multiple invalid login attempt lockouts
  - Tenant-specific audit log tracks all software activity with User Id and IP address logging
  - Session timeout warnings and auto-logout after 30 minutes of inactivity
  - Separate tenant database architecture logically isolates client data
  - Secure authentication and authorization using Microsoft Identity Management
  - SQL Database encryption protects and encrypts all data “at rest”
  - SSL 2048 bit SHA-2 encryption (https) ensures secure transmission of data over the Internet

- Password Security Policy
  - Minimum 8 characters, 1 upper, 1 lower, 1 number, 1 special character
  - Auto-Lockout for 5 minutes after 5 invalid password attempts
  - After 3 auto-lockouts within a 24 hour period, support team is automatically notified via email with support ticket generated

- Two Factor Authentication Security Policy
  - System access/login requires two factor authentication for new computers/browsers not previously registered with browser cookie and unique identifier associated with user account
  - Attempts to pass invalid browser cookie results in notification email sent to tier 2 support for review of security/audit logs for possible blacklisting of IP address where attempt originated from

Neighborly Software

Hosting & Security Frequently Asked Questions

1. Who hosts your software?
   We have partnered with Microsoft Azure and their FedRAMP certified data center for all hosting and infrastructure, which includes web hosting, database hosting and blob storage. Microsoft Azure is recognized as an enterprise-grade cloud computing platform with rigorous standards for security. Our development approach on the Azure platform is to use Microsoft's recommended best practices and managed services for all components of our solution. For example, we use Azure Web Applications and SQL Azure instead of managing those solutions through a cloud hosted VM, therefore adopting Microsoft's added security layer for these solutions.

2. To what geographic locations is it possible for my data to move?
   All Client data is stored, processed, and maintained solely in Microsoft data centers located in the United States.

3. How and where does your company encrypt data at rest and data in motion?
   All client data is encrypted at rest in Microsoft SQL Azure and Azure Storage using FIPS 140-2 validated 256 bit AES encryption. Data is encrypted during transmission by using SSL 2048 bit SHA-2 (https) encryption.

4. Do your company undergo 3rd party audits to validate security?
   Neighborly Software conducts regular 3rd party assessments to protect against unauthorized access including OWASP Top 10 security vulnerabilities.

5. Are backups of my data moved offsite and are they encrypted?
   Data backups are managed securely in the Microsoft cloud using SQL Azure. All backups are encrypted.

6. How does your company ensure my data is not lost or destroyed?
   All client databases are separate and unique to the tenant. In addition, all client databases are backed up on an automated basis and leverage Microsoft SQL Azure which provides Point In Time Restore to any point within the last 35 days. Additional information on this question can be found in the contract, Exhibit A Section 4: "Backup and Recovery of Customer Data. As a part of the Services, Company is responsible for maintaining a backup of Customer Data and for an orderly and timely recovery of such data in the event that the Services may be interrupted. Company shall maintain a contemporaneous backup of Customer Data that can be recovered within four (4) hours at any point in time."

7. How do I get my data if the contract is terminated?
   The following provision is included in our standard contract: "5.4 Upon the termination of this Agreement Company shall, within five (5) business day following the termination of this Agreement, provide Customer, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Service Provider), with a final extract of the Customer Data in electronic format. Further, Company shall certify to

Customer the destruction of any Customer Data within the possession or control of Company, but such destruction shall occur only after the Customer Data has been returned to Customer."

8. How does your company securely delete or destroy my data when requested?
   Upon written request, and confirmed verbally with an authorized Client representative, Neighborly Software will delete the Client-specific SQL Azure database and Azure Storage container in a manner that is non-retrievable.

9. What are your company's notification policies and procedures after a security event?
   Exhibit A, Section 6 of the contract best addresses this question. "5. Loss of Data. In the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of Customer Data or the physical, technical, administrative, or organizational safeguards put in place by Company that relate to the protection of the security, confidentiality, or integrity of Customer Data, Company shall, as applicable: (a) notify Customer as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with Customer in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by Customer; (c) in the case of PII, at Customer's sole election, (i) notify the affected individuals who comprise the PII as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for six (6) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; Notification to affected individuals, as described above, shall comply with applicable law, be written in plain language, and contain, at a minimum: name and contact information of Company's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Company has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Company. This Section shall survive the termination of this Agreement."

10. What happens to my data if your company is purchased by another company?
    All standard contract provisions survive in the event of an acquisition. Section 3 of the contract provides additional detail on Confidentiality and Proprietary Rights.

11. What insurance do your company have to cover a data breach?
    Section 9 of our standard agreement states. "9.1 During the course of performing services under this Agreement, Company agrees to maintain the following levels of insurance: (a) Commercial General Liability of at least $1,000,000; (b) Professional Liability (E&O) of at least $5,000,000; (c) Cyber Liability of at least $5,000,000; and (d). Workers Compensation complying with applicable statutory requirements. Company will add Customer as an additional insured to our Commercial General Liability policy. Company will provide Customer with copies of certificates of insurance upon Customer's written request."