MuniReg Data Security Policy

Effective Date: 01July2023

Policy Owner: MuniReg (Jim Floss, Lead Developer)

Policy Review Date: 01August2023

1. Purpose

The purpose of this Data Security Policy is to identify established guidelines and procedures for safeguarding sensitive data, maintaining data integrity, and ensuring compliance with applicable data protection laws and regulations as they pertain to the web-based MuniReg property registration web tool (aka “application”).

2. Scope

This policy applies to all employees, contractors, and third parties who have access to MuniReg's data, whether stored electronically or in hard copy.

3. Definitions

3.1 Sensitive Data: Any information that, if disclosed or compromised, could harm MuniReg, its customers, or its partners. This includes but is not limited to, personal information, financial data, trade secrets, and proprietary information.

3.2 Data Owner: The individual or department responsible for the creation, maintenance, and protection of specific data sets.

4. Data Classification

Data shall be classified based on its sensitivity and criticality:

Public Data: Information that can be freely shared with the public without any risk to the organization.
Internal Data: Information for internal use only, not to be disclosed outside the organization.
Confidential Data: Highly sensitive information that requires strict access controls and protection measures.

5. Data Handling

5.1 Data Access

Access to data is controlled by user accounts and the assigning of data to said accounts. User accounts are provided user roles to further limit or grant access to data depending on the user role. The User roles are as follows:

- Super Admin (MuniReg and Tech Support Only)
- Employee (Admin & Non-Admin) (MuniReg Employees Only)
- Municipality
- Registering Party

5.2 Data Transmission

Data transmission is conducted over SSL/TLS to encrypt communications between the application and the MySQL Database as well as between the application and third-party applications, such as Stripe.

5.3 Data Storage

Database data is encrypted while at rest using MySQL's built-in encryption features or external encryption tools. Sensitive information, such as credit card information is stored on the Stripe servers with only a customer ID stored locally to identify this information during transactions. All transactions occur over SSL/TLS to ensure the data is encrypted during transmission.

To learn more about the security measures put in place by Stripe please reference this web page.

6. Data Security Measures

6.1 Passwords and Authentication

The use of strong passwords is strongly encouraged by all account holders with a 90-day password update suggestion that occurs for all accounts.

6.2 Data Encryption

Passwords are stored locally utilizing an MD5 hashing algorithm to encrypt the data. All payment information is stored in Stripe, not locally.

6.4 Incident Response

- **Backup:** All data is backed up daily with the code backed up in a remote repository.
- **Recovery:** Data and access can be restored in a matter of minutes.
- **Response and Monitoring:** The application is monitored 24hrs a day through automatic testing means. These automated monitoring and alerting systems (e.g., Uptime Robot, New Relic) help the team to identify and respond to issues in production.

7. Compliance

This application complies with all applicable (US) privacy and data protection laws and regulations. The application is intended for use exclusively by municipalities and their users for registration of US addresses and properties, and accessed on US-based networks.

This application is actively monitored and tested on a weekly basis for security compliance.

8. Review and Revision

This policy will be reviewed annually or as needed to ensure its effectiveness and relevance.

9. Contact Information

For questions or concerns regarding this policy, please contact info@munireg.com