Information Security Policy

Approved: 2025-03-18

Motioned by Commissioner Van Kroonenburg

"I move that Village of Bible Hill adopt the Information Security Policy as presented."

Seconded by Commissioner Pitcher

Motion carried

Purpose and Scope

1. This policy defines security guidelines for the proper handling and protection of sensitive financial information. It aims to ensure the confidentiality, integrity, security, and limited availability of such data.

2. This policy applies to all employees, contractors, and any other third parties who access or manage customer data.

3. This policy is a requirement for Payment Card Industry Data Security Standard (PCI DSS) compliance, by reason of the Village accepting, processing, storing, or transmitting cardholder data using online payment software.

Definitions

4. "Amilia" means Amilia SmartRec, an online recreation programming registration and payment software, including its associated payment processor; and

5. "cardholder data" means sensitive customer payment information such as debit and credit card numbers; and

6. "customer data" means sensitive customer personal information, as defined in Part XX of the Municipal Government Act; and

7. "data" means both cardholder data and customer data.

Payment Processing

8. Electronic payments for Village services may be processed by Amilia. Staff shall not otherwise handle or store cardholder data.

Information Security

9. Access to Amilia shall be provided on a need-to-know basis. All data shall be treated as confidential and shall not be shared with third parties, except for instructors or staff providing services in which the customer is registered, unless agreed to by the customer in writing or otherwise required by law.

10. Staff may export data from Amilia only when required for the performance of one's role. Exported data must be securely stored. Hard copies of data may only be produced given the authorization of the Director of Parks and Recreation or Clerk and Treasurer and shredded when no longer required.

11. Village devices (i.e. computers, mobile devices) used to access Amilia shall be password-protected and have up-to-date anti-virus software.

12. Amilia administration account(s) of Village staff shall be:
    a. limited to only permit access required for the performance of one's role;
    b. password protected; and
    c. protected by multi-factor authentication.

13. Staff shall ensure Village devices are secure and not left logged-in and unattended.

14. Staff shall not share Amilia login credentials.

Reporting Issues

15. Suspected unusual activity or unauthorized access involving Amilia shall be reported immediately to the Clerk and Treasurer or the Audit Committee as the circumstances demand.

Data Destruction

16. Customer data should only be kept for as long as necessary and securely deleted when no longer needed.
17. The Administrative Services Coordinator shall ensure that Amilia client accounts older than 5 years without purchase activity will be deleted on an annual basis.

Policy Document Attestation

Date of notice to Village Commission of intent to consider: 2025-03-11
Date of adoption: 2025-03-18

I certify that this Policy was adopted by Village Commission as documented above:

Chair

March 31, 2025

Date

Clerk and Treasurer

2025-03-31

Date