Information Security Policy Document

Crumbless Keyword Plugin Tool

Document Version: 1.0
Effective Date: 01 August 2024
Review Date: 01 February 2025
Document Owner: Oliver Pearn - CEO

1. Purpose

The purpose of this Information Security Policy is to establish and maintain the security of the Crumbless Keyword Plugin Tool, ensuring the protection of all data associated with the tool against unauthorized access, alteration, disclosure, or destruction.

2. Scope

This policy applies to all systems, employees, contractors, and processes that operate, manage, or support the Crumbless Keyword Plugin Tool. It covers all forms of data, including but not limited to, electronic and physical data.

3. Information Security Objectives

- **Confidentiality:** Ensure that data is accessible only to those authorized to have access.
- **Integrity:** Safeguard the accuracy and completeness of information and processing methods.
- **Availability:** Ensure that authorized users have access to relevant data when needed.

4. Risk Management

- Conduct periodic risk assessments to identify, quantify, and prioritize risks associated with information security.
- Implement appropriate risk treatment plans to mitigate identified risks to an acceptable level.
- Continuously monitor and review the risk environment to adapt controls in response to changes.

5. Asset Management

- Maintain a comprehensive inventory of all information assets associated with the Crumbless Keyword Plugin Tool.
- Classify information assets according to their sensitivity and criticality to the business operations.
- Assign roles and responsibilities for the management of information assets.

6. User Access Management

- Ensure proper company identification and authentication controls for accessing the Crumbless Keyword Plugin Tool.
- Regularly review and revoke company wide access as necessary.

7. Physical and Environmental Security

- Protect physical and virtual environments against unauthorized access, damage, and interference.
- Secure facilities and equipment hosting the service, ensuring proper environmental controls are in place.

8. Operations Security

- Establish secure development practices for the maintenance and development of the Crumbless Keyword Plugin Tool.
- Implement change management procedures to handle changes in a controlled manner.
- Use protection mechanisms against malware.

9. Communications Security

- Encrypt all data transmissions using industry-standard encryption protocols.
- Secure all communication channels, including email and file transfers, to prevent interception, interruption, or modification.

10. Incident Management

- Establish an incident response and management process to handle security breaches or potential security incidents.
- Regularly test and update the incident response plan to ensure its effectiveness in managing and mitigating incidents.

11. Business Continuity Management

- Develop and maintain a business continuity plan to protect, maintain, and recover business-critical processes and systems.
- Conduct regular business impact analyses to identify essential business functions and the resources they require.

12. Compliance

- Comply with applicable legal, statutory, regulatory, and contractual obligations.
- Implement audit and compliance checks to ensure adherence to internal security policies and external requirements.

13. Training and Awareness

- Provide ongoing security training and awareness programs for all employees and contractors to enhance security knowledge and compliance.
- Regularly update training programs to address emerging security threats and updates to security practices.

14. Policy Review and Evaluation

- Regularly review and update the InfoSec policy and associated security measures.
- Ensure the policy remains effective in addressing the threats and challenges faced by the Crumbless Keyword Plugin Tool.