DATA PROTECTION AND INFORMATION SECURITY POLICY

---

1. Introduction

The Stranger Co. recognizes the importance of protecting customer information and maintaining the confidentiality, integrity, and availability of data entrusted to us.

We implement multiple layers of technical security measures to help safeguard customer data, protect our infrastructure, and reduce the risk of unauthorized access, malicious activity, and data exposure.

This document outlines the key security mechanisms used within our environment to protect our systems and support the secure handling of customer information.

2. Security Measures Implemented

2.1 Monarax Malware Scanner

We use the Monarax Malware Scanner to help detect malicious files, suspicious code, and potential malware threats within the hosting environment.

This security measure supports the identification of potentially harmful files and helps reduce the risk of malware affecting our systems and applications.

2.2 Monarax Threat Shield

Monarax Threat Shield is used as an additional layer of protection against potential security threats.

Depending on the capabilities and configuration of the service, it helps support the detection and mitigation of suspicious activity and potential attacks.

Together with other security controls, it contributes to a layered approach to infrastructure protection.

2.3 IP Blocking and Access Restrictions

IP blocking is used to restrict access from specified IP addresses or sources identified as unauthorized or potentially malicious.

This control helps reduce unwanted access attempts and allows access restrictions to be applied where required.

2.4 SSL/TLS Encryption

SSL/TLS encryption is used to help protect data transmitted between users' browsers and our systems.

Our stated configuration uses RSA 2048-bit keys for the relevant TLS certificates or key exchange, as applicable to the deployed configuration.

Encryption helps protect information in transit against interception and unauthorized disclosure. The level of protection also depends on the TLS protocol versions, cipher suites, certificate configuration, and server settings in use.

2.5 Hotlink Protection

Hotlink protection helps prevent external websites from directly embedding or loading protected resources hosted on our server without authorization, where the applicable protection rules are configured.

This measure helps reduce unauthorized use of hosted resources and unnecessary bandwidth consumption.

2.6 Leech Protection

Leech protection helps restrict unauthorized sharing or reuse of protected links, particularly links to password-protected directories or resources, where supported by the hosting configuration.

This measure helps reduce the risk of unauthorized access to restricted content through shared credentials or links.

2.7 Database Username and Password Protection

Database access is protected through authentication using database usernames and passwords.

Access credentials are intended to restrict database access to authorized users and applications. Appropriate database permissions should be assigned according to operational requirements and the principle of least privilege.

Database credentials must be kept confidential and must not be exposed in publicly accessible files, source code repositories, or client-facing documentation.

3. Customer Data Handling

Customer information is handled with the objective of maintaining confidentiality and preventing unauthorized access, disclosure, alteration, or loss.

Our technical security measures support this objective through the following controls:

- **Access Control:** Restricting access through configured authentication and access-control mechanisms.
- **Secure Transmission:** Using SSL/TLS encryption to help protect information transmitted over supported connections.
- **Threat Protection:** Using malware scanning and threat-protection mechanisms to help identify potential security risks.
- **Resource Protection:** Applying hotlink and leech protection where applicable.
- **Database Security:** Using authenticated database access and appropriate permissions.

Customer data should be accessed and processed only for authorized business and service-related purposes, subject to applicable contractual obligations and operational requirements.

4. Security Responsibilities and Best Practices

To maintain an effective security posture, the following practices are recommended and should be followed where applicable:

- Use strong, unique passwords for administrative and database accounts.
- Restrict access privileges to the minimum required for each role or function.
- Keep server software, applications, and dependencies updated.
- Review access permissions and security configurations periodically.
- Maintain appropriate backups and test recovery procedures.
- Monitor available security logs and investigate suspicious activity.
- Follow applicable incident-response procedures if a security event is identified.

These practices help support the ongoing protection of systems, infrastructure, and customer information.

5. Scope and Limitations

The security measures described in this document are designed to reduce security risks and support the protection of customer data. However, no individual security control or combination of controls can guarantee complete protection against every possible threat.

The specific level of protection provided depends on the deployed configuration, service capabilities, access policies, maintenance practices, and operational procedures.

This document describes the security controls identified for our environment. It does not, by itself, constitute an independent security audit, penetration-test report, or certification of compliance with any particular data-protection or information-security standard.

6. Commitment to Data Security

The Stranger Co. recognizes data protection as an important part of delivering reliable and secure services.

We aim to maintain appropriate technical and organizational safeguards for customer information and to review our security practices as necessary to address evolving risks and operational requirements.

For questions regarding our data-protection practices or the security measures described in this document, please contact us through our designated contact channel.

Confidentiality Notice

This document is intended for the designated client and authorized recipients. Distribution outside the intended audience should occur only with appropriate authorization.