Website Security Policy

Effective Date: 07/28/2025
Website: www.soniqcx.com

At **SoniqCX**, we take the security of our website, data, and visitors seriously. This Website Security Policy outlines the measures we take to safeguard our systems and the information we collect and manage. By using our website, you agree to this policy and our broader Terms of Service and Privacy Policy.

---

1. Website Protection Measures

We implement a variety of technical and organizational security measures to protect our website and user data, including:

- **HTTPS/SSL Encryption**: All website traffic is encrypted using Secure Socket Layer (SSL) to ensure secure data transmission.
- **Firewall & Threat Monitoring**: Our hosting environment includes web application firewalls (WAFs), intrusion detection, and automated monitoring to detect and block malicious activity.
- **Secure Hosting**: Our website is hosted in a secure, U.S.-based data center that complies with modern security and infrastructure standards.
- **Software Updates**: We regularly apply security patches and updates to our website platform, content management system, and plugins to reduce vulnerabilities.
- **Access Controls**: Administrative access to the website is restricted to authorized personnel and secured with strong passwords and, where applicable, multi-factor authentication (MFA).

---

2. User Data Security

We protect the limited personal data collected through our website (e.g., contact form submissions) by:

- Encrypting data in transit via HTTPS
- Storing it in secure environments with limited access
- Not collecting sensitive financial or medical information via the site

---

3. Incident Response

In the unlikely event of a website security breach or data incident:

- We will investigate immediately upon detection
- We will contain and remediate the issue as quickly as possible
- If personal information has been compromised, we will notify affected users in accordance with applicable data protection laws

---

4. Responsible Disclosure

We welcome reports from security researchers and the public. If you discover a potential vulnerability on our site, please report it by emailing us at [Insert Contact Email] with the subject line: “Security Vulnerability Disclosure.”

Please include:

- Description of the vulnerability
- Steps to reproduce
- Your contact information (optional for anonymity)

We will review all reports promptly and act where necessary.

---

5. User Responsibility

While we take every reasonable measure to protect our systems, we also encourage users to take precautions:

- Avoid submitting sensitive information through unsecured channels
- Use strong, unique passwords when interacting with any client portal or system provided by SoniqCX
- Report any suspicious emails or phishing attempts claiming to be from SoniqCX

---

6. Policy Updates

We may update this policy from time to time to reflect new threats, technologies, or regulatory requirements. Any changes will be posted to this page with an updated Effective Date.

---

7. Contact

For questions or concerns about website security, please contact:

SoniqCX
Salt Lake City, Ut
Email: justin@soniqcx.com
Website: www.soniqcx.com