Organizational Security

Cipher Tech maintains an Information Security Program that strictly adheres to the criteria set forth by the SOC 2 Framework[1]. This policy includes, but is not limited to, the following components:

- Access Security

  - Permissions and Authentication

    - Access to sensitive information is limited to authorized employees who require it to perform their official duties.

    - Information security measures conform to the highest industry standards.

  - Least Privilege Access Control

    - We follow the principle of *least privilege* with respect to identity and access management.

- Commercial Vendor and Risk Management

  - All commercial vendors are reviewed prior to engagement. Furthermore, Cipher Tech undertakes periodic risk assessments to identify potential threats among our commercial vendors, including considerations for compromise, information theft and fraud.

- Security Awareness Training

  - All employees are required to complete relevant security training covering standard practices, insider threat, and information security topics during onboarding and annually thereafter.

- Confidentiality

  - All employees, consultants, subcontractors, and partners are required to sign and adhere to an industry standard confidentiality agreements prior to their first day of work.

- Background Checks

  - All employees undergo extensive background checks before hiring.

- Network Security

  - Cipher Tech maintains a network security policy that adheres to the SOC 2 Framework, that includes but is not limited to:

[1] SOC 2 is a widely known information security auditing procedure created by the American Institute of Certified Public Accountants.

- **Cloud Infrastructure and Data Hosting Security**

  - Cipher Tech cloud-hosted services/data reside strictly within US cloud-hosting providers who themselves employ robust security programs. For more information and additional details on our cloud security posture, interested ACCE customers may inquire with their customer service representative.

- **Encryption**

  - We employ industry standard encryption algorithms and best practices for handling sensitive data both while at rest and in motion.

- **Logging and Monitoring**

  - We actively log and monitor our networks.

- **Business Continuity and Disaster Recovery**

  - For cloud offerings, Cipher Tech leverages our data hosting provider's backup services to reduce any risk of data loss in the event of a hardware failure. We utilize monitoring services to alert the team in the event of any failures affecting users.

- **Incident Response**

  - We have a process for handling information security events which includes escalation procedures, mitigation and communication.

Contact Us

If you have any questions, comments or concerns or if you wish to report a potential security issue, please contact public@ciphertechsolutions.com.

[1] SOC 2 is a widely known information security auditing procedure created by the American Institute of Certified Public Accountants.