Solve IT Solutions, LLC
Security Statement

Commitment to Security and Privacy

501 N Park Road | Wyomissing, PA 19610 | 484.331.1083

www.solve-it-sol.com

At Solve IT Solutions, we recognize that security is most important to our clients and partners. Our commitment to providing exceptional managed services is matched by our dedication to maintaining the highest standards of security. This statement outlines the principles and measures we employ to ensure the confidentiality, integrity, and availability of the sensitive information and systems entrusted to us.

This Security Statement is aimed at providing you with more information about our security infrastructure and practices. Our Privacy Policy contains more information on how we handle the data that we collect.

Core Principles

Our security framework is built on the following core principles:

- **Confidentiality**: We safeguard sensitive information from unauthorized access and disclosure
- **Integrity:** We ensure the accuracy and completeness of data and maintain reliable systems
- **Availability:** We guarantee that information and services are accessible to authorized users when needed
- **Compliance:** We adhere to all relevant industry standards, regulations, and legal requirements

Security Measures

We employ a multi-layered approach to security, incorporating the following measures:

1.Physical Security

Our data centers and facilities are protected by robust physical security controls, including:

- 24/7 surveillance and monitoring
- Access control systems with biometric or key card verification
- Environmental controls to prevent unauthorized physical access and ensure optimal operating conditions

2.Network Security

We implement advanced network security measures to safeguard our infrastructure and client data:

- Firewalls and intrusion detection/prevention systems
- Encryption for data in transit and at rest
- Regular vulnerability assessments and penetration testing
- Secure and segmented network architecture

3.Endpoint Security

Our endpoint security strategies involve:

- Regular updates and patch management for all devices
- Advanced threat protection and endpoint detection and response (EDR) solutions for all servers and workstations

4.Personnel Security

Solve IT employees are required to conduct themselves in a manner consistent with the company's guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees are required to sign confidentiality agreements and to acknowledge the Solve IT Solutions code of conduct policy. The code of conduct policy outlines the company's expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors.

In addition, all Solve IT employees are required to pass extensive background checks to be eligible for employment with our organization. Additional background checks are performed in areas where required by client industry. These additional background checks include but are not limited to:

- PA Criminal History
- PA Child Abuse
- FBI Fingerprinting
- Criminal Justice Information Services (CJIS)

5.Access Control

We maintain strict access control policies to ensure that only authorized personnel can access sensitive information:

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Regular access reviews and audits
- Principle of least privilege applied to all users and systems

6.Data Protection

Our data protection practices include:

- Regular data backups and secure storage solutions
- Data loss prevention (DLP) technologies
- Comprehensive data lifecycle management
- Compliance with data protection regulations such as GDPR, CMMC, and HIPAA

7.Incident Response

We have a robust incident response plan to address potential security incidents promptly and effectively:

- Dedicated incident response team
- Regular training and simulation exercises
- Clear communication protocols and escalation procedures
- Post-incident analysis and continuous improvement

8.Employee Training and Awareness

We ensure that our employees are well-versed in security best practices through:

- Regular security awareness training programs
- Phishing simulation exercises
- Clear security policies and guidelines
- Encouraging a culture of security within the organization

9.Supplier and Vendor Relationships

Solve IT partners with suppliers and vendors that operate with the same or similar values around lawfulness, ethics, and integrity that Solve IT does. As part of its review process, Solve IT screens our suppliers and vendors and binds them to appropriate confidentiality and security obligations, including requirements for appropriate management of any customer data they may handle.

10.Compliance and Audits

To ensure adherence to the highest standards, we engage in regular compliance activities:

- Internal and external audits
- Third-party assessments and certifications
- Continuous monitoring and improvement of security practices

Conclusion

At Solve IT Solutions, we understand that trust is earned through consistent performance and unwavering commitment to security. Our comprehensive security measures are designed to protect the interests of our clients and ensure that their data and systems remain secure. We continuously evaluate and enhance our security practices to stay ahead of emerging threats and maintain our position as a trusted Managed Service Provider.

For any questions or further information about our security practices, please do not hesitate to contact your dedicated account manager.