SOLENIS INFORMATION SECURITY ADDENDUM

This Information Security Addendum outlines the security controls and practices implemented by Solenis to protect employees, contractors, and customer data within its hosted services. It forms part of the agreement between the parties and is intended to ensure transparency and alignment on data protection and risk management. This addendum may be updated periodically, with changes effective upon publication.

1. Governance
    a. Digital Security Organization

        The Solenis Digital Security Organization (DSO) reports to the Senior Vice President of IT and Chief Information Officer (CIO) and interfaces with cross-functional internal teams to coordinate Solenis security resilience.

        Our mission is to ensure a safe and successful business environment for our teams and customers by combining the right people, processes, and technology.

        The Digital Security Program's main objectives are:

        i. Protect Data and Critical Assets
        ii. Manage Cyber Risks and Threats Proactively
        iii. Ensure Resilience and Incident Preparedness
        iv. Promote a Security-First Culture
        v. Maintain Compliance and Governance

    b. Policies

        Selected Solenis policies or standards applicable to cybersecurity incident response, preparedness, and/or resilience:

        i. Acceptable use
        ii. Email policy
        iii. Risk Management Policy
        iv. Human Resource Security Policy
        v. Business Continuity and Disaster Recovery Plan
        vi. Cryptography Policy
        vii. Compliance policy
        viii. Asset Management Policy
        ix. Incident Response Plan
        x. Information Security Policy
        xi. Bring your own device policy
        xii. Operations Security Policy
        xiii. Physical Security Policy
        xiv. Access Control Policy
        xv. Third-Party Management Policy
        xvi. Clean desk clear screen policy
        xvii. Information Security Training Policy
        xviii. Change management policy
        xix. Backup and Restore policy
        xx. Email Retention policy
        xxi. Job Management

c. Certifications and Audits
    i. Solenis conducts annual internal audit of its information security controls and information technology as a part of its compliance with the Sarbanes-Oxley Act.
    ii. Solenis holds ISO/IEC 27001 certification for its information security management system, as well as SOC 2 Type 1 attestation, demonstrating our commitment to maintaining rigorous security controls and protecting customer data.

2. Risk Management

a. Third-party Risk Management: Solenis maintains a Third-Party Risk Management (TPRM) program to evaluate the security practices of its vendors. As part of this process, vendors are required to implement appropriate information security controls and practices. Hosting providers must maintain security measures that are, at a minimum, aligned with SOC 2 standards.

b. The Awareness Program
    i. Ongoing Security Awareness and Training:
    Solenis delivers quarterly mandatory digital security training through its Learning Management System (LMS), continuously updating content to keep employees and contractors informed. This is reinforced with simulated phishing exercises conducted quarterly to enhance vigilance against the leading cyberattack vector—malicious emails.

    ii. Continuous Engagement and Communication:
    To maintain cybersecurity awareness, Solenis uses multilingual screensavers with best practice reminders and actively updates its Digital Security section on the company intranet with relevant tips, guides, and collaborative content tailored to employee needs. The Digital Security Office (DSO) also works closely with communications teams, contributing content for ad-hoc communications on emerging threats such as smishing (SMS phishing) and vishing (voice phishing), helping employees protect themselves and the organization.

c. Change Management: Solenis adheres to a structured change management process for administering modifications to production and non-production environments, including updates to software and infrastructure. All changes are subject to review and validation in a test environment prior to deployment in production.

d. Contingency Planning: Solenis maintains and administers disaster recovery and business continuity plans to minimize the impact of disruptive events on the delivery and support of its business. These plans are tested as part of Solenis internal audits and security assessments.

e. Software Vulnerability Management

Solenis uses a reactive and proactive software vulnerability management process.

i. Reactive: open-source and vendor research is conducted by the members of the DSO team to learn of any new vulnerabilities reported and unreported in any of the platforms, software or hardware, in use globally at Solenis. Identified and confirmed vulnerabilities are rated and addressed through either software patching or mitigating controls, in the absence of software patches.
ii. Proactive: scheduled and automated weekly scans of all platforms are conducted, and results are addressed based on risk. Critical vulnerabilities (those with critical CVSS, active exploit, and no mitigations in place) are addressed immediately. Every other identified vulnerability is addressed in a time window of 5 (five) to 30 (thirty) days, depending on criticality and affected systems.
iii. Secure Coding Practices: Solenis develops software using secure software development lifecycle practices that align with industry-standard frameworks, such as the OWASP Top Ten or a substantially equivalent standard. These practices are integrated into the software development lifecycle to help identify and mitigate security vulnerabilities.

f. Internal and External Audit
   i. Regular External Audits and Security Assessments:
   Solenis undergoes periodic IT and financial audits by internal and external auditors, covering almost 430 controls including access management, change management, user access review, job monitoring, and backup and recovery.

   ii. Proactive Cybersecurity Monitoring and Testing:
   Solenis maintains a strong cybersecurity posture through continuous monitoring of external security ratings and internal KPIs. The DSO collaborates with top-tier external firms for regular penetration testing. The DSO works collaboratively with these firms to remediate findings as soon as they are identified, or shortly thereafter.

3. Cybersecurity Posture

Prevention and Detection Toolset

- The DSO manages a yearly capital and operation budget that is approved by Solenis' Executive Committee to further strengthen our posture, improve resiliency and reduce cybersecurity risks.
- Strategic investments are made in people, processes and technologies to ensure the DSO achieves its mission.

Areas we focus on with examples of technologies and processes in use at Solenis:

a. Data Protection:
   i. Solenis maintains a comprehensive data protection strategy that includes data loss prevention, a robust data security program, behavioral analytics, advanced email malware and URL protections, and integrated data privacy governance, with the Chief Information Security Officer (CISO) actively participating in the Data Privacy Office. (DPO)

b. Endpoint Protection:
    i. Secure Endpoint Access and Management:
    Solenis enforces VPN connections secured with two-factor authentication and implements internet content filtering to block malicious sites, while centrally managing endpoints—including desktops, laptops, and mobile devices—through unified endpoint management.

    ii. Robust Endpoint Security Controls:
    Local administration privileges are removed or tightly controlled with unique, rotating passwords; disk encryption is centrally managed based on risk; and ongoing vulnerability management ensures continuous protection across all endpoints.

c. Server Protection:
    i. Secure Administrative Access:
        Administrators must use multi-factor authentication to connect to all on-premises and cloud servers, accessing infrastructure only through purpose-built, hardened jump desktops to minimize risk.

    ii. Controlled and Hardened Infrastructure:
        Solenis enforces broad internet access restrictions on all servers and utilizes hardened golden images for Windows and Linux, based on CIS benchmarks and industry best practices.

    iii. Centralized and Automated Management:
        System administration is managed centrally with Infrastructure-as-Code automation, complemented by proactive vulnerability management to ensure continuous security and compliance.

d. Global Network Protection:
    i. Solenis employs a global SD-WAN built on Secure Access Service Edge (SASE) architecture that enforces policy-based security, network segmentation with role-based access controls, and global Network Access Control (NAC) to ensure only approved users and devices securely access appropriate applications and data.

e. Identity Protection:
    i. Modern Identity and Access Management:
        Solenis uses a modern identity provider with mandatory SAML 2.0 authentication for all applications, gradually phasing out legacy Active Directory integrations to enhance security and streamline access.

    ii. Strong Authentication and Least-Privilege Access:
        All employee and contractor accounts are secured with next-generation multi-factor authentication, and access to business-critical applications is strictly governed by Role-Based Access Control (RBAC) following the least-privilege.

f. Cloud Protection:
    i. Solenis operates a secure hybrid cloud environment— with public cloud infrastructure for IaaS and PaaS—governed by standardized cybersecurity controls and increasingly automated through Infrastructure-as-Code and continuous configuration monitoring.

g. Cybersecurity Incident Response

    i. Proactive Threat Monitoring and Detection:
        Solenis operates a dedicated Security Operations Center (SOC) that continuously monitors infrastructure, systems, and applications using real-time tools, SIEM platforms, and AI-driven threat detection. By leveraging behavior analytics, threat intelligence feeds, and anomaly detection, the SOC rapidly identifies and prioritizes high-risk incidents.

    ii. Automated Response and Continuous Improvement:
        The SOC utilizes Security Orchestration, Automation, and Response (SOAR) tools to streamline alert triage and automate remediation workflows. Its effectiveness is continuously enhanced through regular red team exercises, internal simulations, and feedback loops that refine detection rules, response playbooks, and overall incident readiness.

h. Physical Security

    i. Secure areas:
        Physical access shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Access cards are used for entry and exit of premises. Users can only access through the access cards.