SOLENIS

Solenis Digital Security, Briefly Stated

Solenis' most important concerns are the resilience of our operation and protection and reliability of our data. Our digital security mission is to ensure a safe and successful business environment for our teams and customers by combining the right people, processes, and technology.

In short, we:

- Employ the latest cyber security prevention and detection techniques with a globally distributed team of highly skilled experts.
- Have an evolving security model that helps us understand and respond to the ever-changing threat landscape.
- Prioritize protecting our digital assets with an equal focus on the digital assets of our partners.
- Audit and programmatically respond to identified vulnerabilities.
- Educate all our employees, contractors, and our Board of Directors.
- Balance risk, trust, and opportunity in an uncertain world.

Key elements of our digital security program

Solenis' digital security program governance assures that we have the correct information structure, leadership and guidance. Ethics helps us ensure we act morally and reasonably. Our risk analysis process ensures we identify, analyze and mitigate risk. This is accomplished through the development and enforcement of documented policies, standards, requirement and various reporting metrics.

The primary objective of Solenis' security awareness program is the keen awareness, on the part of all employees and contractors, of the reality of the different types of attacks that we may be subject to, together with knowledge of what Solenis expects them to do in various situations. Further, employees and contractors are to understand and comply with Solenis' Acceptable Use policy, Information Security policy, Data Protection policy, and other applicable policies.

The purpose of Solenis' third-party risk management processes is to identify and remediate risks associated with third parties. The techniques used serve to extend our risk management function to include methods of identifying various types of risks introduced because of a digital connections and relationship with third parties.

We examine information systems (including but not limited to operating systems, subsystems such as database management systems, applications, and network devices) for the purpose of discovering exploitable vulnerabilities, related analysis, and make decisions about remediation. Solenis employs vulnerability management as a primary activity to reduce the likelihood of successful attacks on our IT environment.

Through identity and access management (IAM) we manage the identities of workers and systems, as well as their access to systems and information. Solenis manages the identity and access history of each employee, contractor, temporary worker, supplier worker and, sometimes, customer. These records are then used as the basis for controlling which workplaces, applications, IT systems and business functions each person is permitted to use.

Solenis undertakes disaster recovery planning to reduce risks related to the onset of disasters and other events. Through DRP we ensure that key IT systems are available to support business processes.

Data security is at the heart of our security program and we correlate it with information security laws and standards. We employ proactive and reactive controls to the areas of access management, encryption, backup and recovery, data loss prevention, cloud access security brokers and user behavior analytics.

Solenis' security incident process is organized, documented, and rehearsed. We investigate all events where the confidentiality, integrity, or availability of information (or an information system) has been or is in danger of being compromised.

Adrian Giboi
Director, Digital Security

###