# Statement of Security
# Our People, Our Process, Our Technology

Spirit maintains the confidentiality, integrity and availability of its information and digital resources through comprehensive and proactive compliance, privacy and risk programs developed from industry accepted best practices. The framework for our programs are based on the Department of Defense Cybersecurity Maturity Model Certification (CMMC) requirements and National Institute of Security and Technology (NIST) frameworks, Generally Accepted Privacy Program (GAPP) guiding principles and ISO 27001/2 standards. They are inclusive of well-informed people, well-defined processes and highly effective technology.

## ***OUR PEOPLE***

The Vice President, Chief Information Security Officer (CISO) and Privacy Officer (PO), reporting to the Executive Vice President and Chief Operating Officer, is responsible for the Global Information Security and Risk Management functions. This includes securing the global data and digital infrastructure of Spirit AeroSystems.

The teams under the CISO/PO oversee all aspects of information security, enterprise risk management, crisis management, business continuity, digital compliance, and data privacy. Organizational, physical and operational security is maintained by a full-time staff of professionals with defined roles and responsibilities of various information, industrial and physical security specialties.

The Director of Trade Compliance, reporting to the Senior Director of Compliance and Sustainability (who reports to the Senior Vice President, Chief Administration and Compliance Officer), is responsible for Spirit's global trade compliance program, creating policy and providing oversight in securing Spirit's export controlled data footprint, including all data export control regulations globally for Spirit AeroSystems.

Spirit AeroSystems takes the safeguarding of information and assets seriously and enforces information security as each employee's responsibility. Spirit AeroSystems ensures employees are placed into positions of trust are honest, reliable and not likely to harm Spirit, its employees, customers, primes or shareholders. Background checks are completed on employees prior to employment, when permitted by applicable law. Spirit also has a robust, multi-departmental insider threat program, in conjunction with its industrial security program.

All employees are required to acknowledge ongoing compliance with Spirit policies and complete continuous awareness training. Policy compliance is reinforced through targeted role-based employee risk awareness training, executed through a variety of delivery channels.

Employees and other individuals working on behalf of Spirit that have access to corporate information resources are required to report violations of Spirit's security policies and standards.

## ***OUR PROCESS***

Spirit has established a formal enterprise risk program developed from industry best practices and frameworks including NIST and the ISO/IEC 27001/2 standard. The program addresses all aspects of enterprise risk, including information security and privacy, and applies policies and standards that ensure appropriate controls are implemented and regulatory compliance observed. Spirit performs regular audits and risk assessments to measure the effectiveness of the program. The CISO participates in quarterly Board meetings to provide status on the enterprise risk program.

The Senior Manager of Global Information Security serves as the coordinator of the Digital Incident Response Team. Global Information Security and Information Technology Teams are chosen based on the required subject matter expertise. Depending on the severity and nature of the incident, various members of the business and Executive Leadership Team are brought into the Digital Incident Response Team.

Spirit's Global Information Security Team directs the formal vulnerability management program, which identifies and prioritizes system and application vulnerabilities based on business risks. The vulnerability management program ensures security patches and critical code updates are applied.

Enterprise Risk Management and Corporate Compliance oversee privacy policies and compliance audits including GDPR, SOX, GLBA, HIPAA, and other relevant country and region-specific cybersecurity and data privacy regulations. Additionally, they assess third-party vendors and contracts to validate compliance with Spirit security policies and controls and external data protection requirements. Further, Spirit maintains a proactive internal audit function that maintains oversight of all aspects of Spirit internal controls, and ensures applicable laws and regulations are followed.

Spirit utilizes internal and third-party resources to ensure mitigation and recovery from events that could interrupt vital business functions. Business continuity and disaster recovery exercises are conducted, and documented plans and playbooks are maintained and validated through proactive tabletop exercises. These exercises confirm the effectiveness of our program. Business continuity plans include: Emergency Management, Incident Management, Crisis Management, Business Continuity, and Disaster Recovery/Contingency Planning.

## ***OUR TECHNOLOGY***

Spirit incorporates processes and technology to control authentication to systems and applications. These controls allow only authorized personnel to access data appropriate to their business need and job function. Employees log on to computing systems with unique user IDs and strong passwords. Two-factor authentication is implemented based on access requirements, privileges needed and criticality of the asset. All privileged

access authentication is performed with a privileged access solution that continuously rotates passwords. Centralized log monitoring and management systems are used for compliance, archival and forensic analysis purposes.

Spirit monitors and controls its corporate network to ensure secure communications, utilizing encryption, network segmentation and firewall technology. Rules for permitting or denying specific network traffic through a firewall are explicitly documented in each device configuration, and all ports are closed, except where there is a specific business need. All firewall rules are vetted through an enterprise firewall change board. All network traffic is closely monitored for suspicious activity and anomalies via internal and third-party managed intrusion protection systems.

Relevant and emerging vulnerabilities are closely tracked by a full-time security staff and a third-party managed security service. PCs, servers, databases, and network devices and web applications are scanned for vulnerabilities on a regular basis, while a defense-in-depth strategy provides layered protection for monitoring, detecting and removing malicious code identified at the gateway, server and desktop layers.

Data loss prevention efforts include: monitoring outbound communications, supporting the protection of email traffic through phishing filtering and malware detection, as well as utilization of data protection and insider threat detection technologies. Mobile devices are encrypted, and removable media restricted to those with appropriate access to role-based exceptions. Removable media are also encrypted to prevent loss of data.

## ***ADDITIONAL INFORMATION***

This Statement of Security is provided for informational purposes only. It is not intended to be construed or relied upon as legal advice or to have any legal effect. Spirit AeroSystems continuously updates and improves its security infrastructure and practices, which will deviate from those described in this Statement of Security over time.

Please contact us at InformationSecurity@Spiritaero.com for additional information regarding Spirit's security infrastructure and practices.