☐ Restricted ☐ Confidential ☐ Sensitive ☐ Internal Use Only ☒ Public

Date: 14-Sep-2021

Subject: Mirion Technologies: Cybersecurity and Data Protection Program

From: Office of Chief Information Security Officer | Mirion Technologies Inc. | cybersecurity@mirion.com

Mirion will comply with applicable statutory, regulatory, and mutually agreed upon contractual obligations that apply to Mirion; however, Mirion does not assume any obligations to make a customer compliant with applicable statutory and regulatory obligations that may apply to the customer.

Controls Category	Mirion Practice
Governance **(ID.GV)**	**Governance Framework:** Mirion's Cybersecurity and Data Protection program is based on the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF 1.1) and Special Publication (SP) 800:53 Rev 5. **Policies:** Mirion periodically reviews and updates the Cybersecurity Policies and Standards in accordance with industry standards. **Assurance:** Mirion has established periodic, independent assessments to ensure that Cybersecurity Policies, Standards, and Controls are implemented in accordance with internal policy and standards.
Asset Management **(ID.AM)**	**Asset Management:** Mirion maintains an inventory of system and software assets and related configuration metadata. **Asset Classification:** Mirion's information assets are assigned a classification level based on its level of sensitivity and the impact to the organization in order to appropriately restrict access and ensure the appropriate minimum baseline standards (low, medium, high) are implemented in accordance with NIST 800.53 Rev 5.
Risk Assessment **(ID.RA)**	**Vulnerability Management:** Mirion utilizes scanning tools to assess systems, services, and applications on a periodic basis in accordance with internal policies. • Identified vulnerabilities are risk assessed, resolved and/or mitigated in a timely manner in accordance with internal policies. • Ad-hoc scans are performed as necessary when new vulnerabilities are identified that affect Mirion systems, services, and applications • Scanning tools are updated to the latest vulnerability databases on a routine basis in accordance with internal policies **Threat Hunting:** Mirion has established a dedicated security team to proactively search for Indicators of Compromise (IoC) and to detect, track and disrupt threats that evade existing security controls in Mirion systems, applications, and services.
Risk Management Strategy **(ID.RM)**	**Governance Structure:** Mirion has a dedicated group, Digital Security Services (DSS), reporting to the Chief Information Security Officer (CISO), that centrally operates the Cybersecurity and Data Protection Program at an enterprise level to address Mirion's applicable statutory, regulatory, and contractual obligations. Additionally, a dedicated team within the DSS organization manages Cyber Risk, Governance, and Compliance. **Risk Assessment**: Mirion's CISO organization conducts periodic risk assessments and communicates to executive leadership.
Supply Chain Risk Management **(ID.SC)**	**Review of General IT and Security Controls:** Mirion identifies and verifies General IT Controls and Security controls on a recurring basis in accordance with internal policies. This may include reviews based on inquiry, independent audit reports (e.g., SOC 1), or other IT certification documents based on the vendor risk and in accordance with internal policies.

Controls Category	Mirion Practice
Identity Management, Authentication and Access Control **(PR.AC)**	**Identity and Authentication Policy:** Mirion requires proper user identification and authentication management for all standard and privileged users on all systems, applications, and services • Unique user IDs are required • Shared, group, generic, and anonymous end user accounts are specifically prohibited, unless specifically approved by the Office of the CISO. • Authentication mechanisms are based on data classification and system impact. • At a minimum, multi-factor authentication is required for access to Mirion network • Minimum password standards are enforced in accordance with industry standards and internal policy, which include, at a minimum: password length, password complexity, password expiration, password lockout, and password re-use. **Access Control Policy:** Mirion limits access to its systems and data to authorized users. • Documentation of the addition, deletion and modification of user IDs, credentials and other identifier objects is maintained to verify authorized access to Mirion systems and data • User access is revoked timely and in accordance with internal policy to all Mirion systems and data • Appropriate segregation of duties is maintained **Least Privilege:** Mirion restricts access to systems and data to only those individuals who require such access to perform their job function. **Privileged User Accounts:** Privileged user accounts are assigned in accordance with job classification and function and based on a least-privileged approach and "deny all" unless specifically allowed. **Physical Access:** Mirion restricts and monitors access to facilities where information systems are located.
Awareness and Training **(PR.AT)**	**Security Training.** Mirion requires Security Awareness Training for its employees in accordance with internal policy. **Acceptable Use**: Mirion has an established Acceptable Use Policy that governs the acceptable and unacceptable use of computing and communications for accounts, devices, and network resources.
Data Security **(PR.DS**)	**Data Backup:** Mirion backups systems and data on a regular basis in accordance with internal policies. Access to backups is appropriately restricted to authorized personnel. **Data Classification:** Mirion assigns a sensitivity level for data based on the appropriate audience and impact of the system. Regulatory, legal, contractual, and/or company directives supersede standard classification levels. The standard data sensitivities are as follows: restricted, confidential, internal use, and public. **Data Discovery:** Mirion performs periodic data discovery and data classification reviews in accordance with internal policies and regulatory statutes. **Data Encryption**: Mirion encrypts data at-rest and in-transit in accordance with internal policies and data classification.
Information Protection Processes and Procedures **(PR.IP)**	**Secure System Development Life Cycle:** Mirion products and solutions apply product security design guidelines during engineering process in accordance with internal policies. The security standards are designed based on industry best practices and governed by Mirion CISO organization. Product security standards addresses the need of hardware, firmware, operating system, application, data, and network security as appropriate and applicable to product/solution. **System Environments**: Mirion maintains separate development, testing, and production environments. **Pre-Employment Screening:** Appropriate background checks are completed for employees and contractors in prior to employment in accordance with internal policy. **Confidentiality Agreements:** Mirion ensures employees and contractors sign confidentiality agreements in accordance with internal policy. **Security Policy Compliance:** Any person subject to Mirion's Cybersecurity Policies and Standards, who fails to comply with the provisions are subject to appropriate disciplinary or legal action in accordance with the Mirion's Disciplinary Code and Procedures.

Controls Category	Mirion Practice
Threat Intelligence and Incident Management *	**Penetration Testing:** Mirion performs periodic penetration testing on systems, applications, and services in accordance with internal policies. **Event Logging:** Mirion enables system logging, where technologically feasible, of defined events in accordance with internal policies. The logs are centrally managed and monitored on a periodic basis, where potential security issues are investigated and resolved. **Malicious Code:** Mirion Technologies uses security software and technology to protect against malicious code**.** **Security Incident Response Policy:** Mirion has a dedicated security team to assess, mitigate, investigate, document, and report security incidents in accordance with internal policy. • Mirion ensures appropriate incident data collection and notifications in accordance with applicable laws, standards, and internal policy. **Data Retention:** Mirion retains data in accordance with applicable statutory, regulatory, and contractual obligations. Access to off-site storage media is appropriately restricted to authorized individuals. **Data Recovery**: Mirion periodically performs data recovery procedures in accordance with internal policies to ensure data is available and recoverable.

*Includes NIST Security Control Categories: Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, and Recovery Planning

Revision Date	Version No	Description of Change / Sections Affected	By Whom
14–Sep-2021	1.0	First Version	Senior Manager, Cybersecurity & Compliance