Data Processing Addendum ("**Agreement**")

BETWEEN

(1) **Mirion Technologies (GDS), Inc.** incorporated and registered in Delaware with company number 3700491 whose registered office is at c/o Cogency Global Inc., 850 New Burton Road, Ste 201, Dover, DE 19904 USA with mailing address 104 Union Valley Road, Oak Ridge, TN 37830, USA ("**Mirion**"); and

(2) The legal entity that is party to and executed the underlying Services Agreement as a Customer (the "**Customer**").

BACKGROUND

(A) Mirion provides monitoring of individuals for occupational exposure to ionizing radiation and related services ("**Services**") to the Customer pursuant to an agreement ("**Services Agreement**").

(B) This Agreement forms part of and is incorporated by reference into the Services Agreement entered into by the Customer and Mirion concerning Customer's use of the Services to reflect the parties' agreement regarding the Processing of Personal Data in accordance with Data Protection Legislation and sets out the framework for the transferring of Personal Data from the Customer to Mirion to be processed for the purpose of providing the Services.

(C) This Agreement consists of the terms described herein, Schedule 1 and Schedule 2 including any Attachments thereto. By executing the Services Agreement, the parties are agreeing to all parts of this Agreement.

1 Definitions

1.1 In this Agreement

1.1.1 "**Data Protection Legislation**" shall mean the Data Protection Act 2018 (as applicable) and the Regulation (EU) 2016/679 as implemented into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") (as amended, updated or re-enacted from time to time);

1.1.2 "**Standard Contractual Clauses**" shall mean the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR.

1.1.3 "**Data Subject**", "**Controller**", "**International Organisation**", "**Processor**" and "**Processing**" have the same meaning as in the Data Protection Legislation;

1.1.4 "**Personal Data**" has the meaning set out in the Data Protection Legislation.

1.1.1 "**Third Country**" means any country other than the UK, a European Union Member State or a member of the European Economic Area at the time of transfer of Personal Data or a country that is not subject to an adequacy finding by the Information Commissioner's Office ("**ICO**").

2 Data Processing

2.1 For the purposes of the Data Protection Legislation, Mirion is a Processor acting on behalf of the Customer, who is the Controller of the Personal Data.

2.2 The nature, purpose and duration of the Processing, the categories of Personal Data and the categories of Data Subjects whose Personal Data is being Processed in connection with the Services are set out in Schedule 1 of this Agreement.

2.3 Mirion shall comply with its obligations under the Data Protection Legislation and shall, in particular:

2.3.1 process the Personal Data only to the extent necessary for the purpose of providing the Services and in accordance with the Customer's written instructions (including with respect to transfers of Personal Data to a Third Country or to an International Organisation);

2.3.2 implement appropriate technical and organisational measures in accordance with the Data Protection Legislation to ensure a level of security appropriate to the risks that are presented by such Processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the

likelihood and severity of risk in relation to the rights and freedoms of the Data Subjects;

2.3.3 ensure that any employees or other persons authorised to Process the Personal Data are subject to appropriate obligations of confidentiality;

2.3.4 on request by the Customer and taking into account the nature of the Processing and the information available to Mirion, assist the Customer in ensuring compliance with its obligations under the Data Protection Legislation in respect of the Personal Data;

2.3.5 engage any third-party sub-processor to carry out its Processing obligations under this Agreement by way of a written contract that such third party will, at all times during the engagement, be subject to data processing obligations equivalent to those set out in this Agreement;

2.3.6 notify the Customer, as soon as reasonably practicable, about any request or complaint received from a Data Subject (without responding to that request, unless authorised to do so by the Customer) and assist the Customer by technical and organisational measures, insofar as possible, for the fulfilment of the Customer's obligations in respect of such requests and complaints;

2.3.7 notify the Customer on becoming aware of a Personal Data breach;

2.3.8 on request by the Customer, make available information necessary to demonstrate the Customer's compliance obligations under the Data Protection Legislation and on reasonable advance notice in writing permit, and contribute to, audits of compliance with Data Protection Legislation and this Agreement carried out by the Customer (or its authorised representative);

2.3.9 on termination or expiry of this Agreement, destroy, delete or return (as the Customer directs) all Personal Data and delete all existing copies of such data unless required by law to keep or store such Personal Data.

2.4 The Customer consents to the engagement sub-processors. This authorization will constitute Customer's prior written consent to the subcontracting by Mirion of the processing of

Personal Data as required under the standard contractual clauses or the Data Protection Legislation.

2.5 Mirion may, from time to time, engage new sub-processors. Mirion will give Customer notice of any new sub-processor at least 30 days in advance of providing that sub-processor with access to Customer Data by updating the website and providing the Customer with a mechanism to obtain notice of that update. The Customer may object to Mirion's use of a new sub-processor by notifying Mirion promptly in writing within ten 10 business days after receipt of Mirion's notice in accordance with the mechanism set out in this Section 2.5. If the Customer does not approve of a new sub-processor, then the Customer may terminate the applicable Agreement(s) without liability with respect only to those Services that cannot be provided by Mirion without the use of the objected-to new sub-processor by providing, before the end of the relevant notice period, written notice of termination.

2.6 The Customer acknowledges that clause 2.3.1 shall not apply to the extent that Mirion is required by law to Process the Personal Data other than in accordance with the Customer's instructions and Mirion acknowledges that, in such a case, it must promptly inform the Customer of the relevant legal requirement prior to Processing unless the law prohibits the provision of such information.

2.7 If Mirion becomes aware that any law enforcement, regulatory, judicial or governmental authority outside the UK (an "**Authority**") wishes to obtain access to or a copy of some or all Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Personal Data to such Authority, Mirion shall:

2.7.1 immediately notify Customer of such Authority's data access request;

2.7.2 inform the Authority that it is a Processor of Personal Data and that Customer has not authorised them to disclose that Personal Data to the Authority;

2.7.3 inform the Authority that any and all requests or demands for access to Personal Data should be notified to or served upon Customer in writing; and

2.7.4 not provide the Authority with access to Personal Data unless and until authorised by Customer.

2.8 In the event Mirion is under a legal prohibition or a mandatory legal compulsion that prevents them from complying with clause 2.7 in full, Mirion shall use reasonable and lawful efforts to challenge such prohibition or compulsion (Customer acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request).

2.9 If Mirion makes a disclosure of Personal Data to an Authority (whether with Customer's authorisation or due to a mandatory legal compulsion) Mirion shall only disclose such Personal Data to the extent Mirion is legally required to do so and in accordance with applicable lawful process.

2.10 Clauses 2.7 to 2.9 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Personal Data, Mirion has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Mirion shall notify Customer as soon as possible following such Authority's access and provide Customer with full details of the same, unless and to the extent Mirion is legally prohibited from doing so.

2.11 Mirion shall not knowingly disclose Personal Data in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

2.12 Mirion shall have in place and maintain in accordance with good industry practice measures to protect Personal Data from interception (including in transit from Customer to Mirion and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit to deny attackers the ability to read data.

3 General

3.1 To allow Mirion to provide the Services the Customer transfers the Personal Data to Mirion and thus to the USA. Accordingly, the parties will be deemed to have entered into the standard contractual clauses set out in Schedule 2 of this Agreement that shall be incorporated into this Agreement and apply to such transfers.

3.1.1 In so far as Schedule 1 applies to Appendix 1 of Schedule 2, Appendix 1 of Schedule 2 shall be deemed to be completed using the details set out at Schedule 1.

3.1.2 It is not the intention of either Party to contradict or restrict any of the provisions set forth in the standard contractual clauses and, accordingly, if there is any conflict between this Agreement and the standard contractual clauses, the standard contractual clauses will prevail.

3.1.3 Mirion may, at any time on not less than 30 days' notice, revise this Agreement by replacing it with any controller to processor standard clauses adopted for transfers of personal data out of the United Kingdom.

3.2 This Agreement shall be governed by the law of the country within the United Kingdom in which the data exporter is established.

Schedule 1

Data Processing

List of parties	
Data exporter	The Party identified as the Controller in the Agreement
Data Importer	Mirion Technologies (GDS), Inc. Edwin Ulbricht, Data Protection Officer privacy@mirion.com
Description of the processing / transfer	
Nature/purpose of Processing	The data importer provides dosimetry services e.g., services to measure and track exposure to ionizing radiation for occupational and other safety purposes. The provision of dosimetry services are the activities relevant to the transfer of personal data. The personal data being transferred pertains to the individual employees covered by the data exporter's radiation monitoring programs and for which data exporter procures dosimetry services from the data importer.
Duration of Processing	For the duration of the Services Agreement.
Categories of Data Subjects	Employees of the data exporter covered by the data exporter's radiation monitoring programs and for which data exporter procures dosimetry services from the data importer.
Categories of Personal Data	• Full name • Gender • Identification numbers as required by applicable regulations • Date of birth • Place of birth • Occupational/Industry category • Start date and end date of monitoring • Email address

Special Categories of Personal Data	Radiation dose. In addition, the personal data may – but does not necessarily - include the pregnancy start and end dates of the data subject.
Third Countries or International Organisations Personal Data will be transferred to	United States of America
Sub-Processors	Cloud-based hosting services are provided by: Rackspace Technology Dallas TX, USA and Frankfurt, Germany Microsoft Corporation, USA

Schedule 2

Standard Contractual Clauses

Name of the data exporting organisation:

The data exporter is the legal entity that executed the Agreement as a Controller/ Data Exporter.

(the data **exporter**)

And

Name of the data importing organisation: Mirion Technologies (GDS), Inc.

Address: 104 Union Valley Road, Oak Ridge, TN 37830, USA

Tel. +1 (949) 419-1000; **fax** N/A; **e-mail:** dsd-support@mirion.com

Other information needed to identify the organisation: None.

(the data **importer**)

Clause 1. Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data

exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3. Third-party beneficiary clause

3(1) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3(2) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3(3) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against

such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3(4) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4. Obligations of the data exporter

The data exporter agrees and warrants:

4(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

4(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

4(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

4(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

4(e) that it will ensure compliance with the security measures;

4(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

4(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

4(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

4(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

4(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5. Obligations of the data importer

The data importer agrees and warrants:

5(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

5(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

5(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

5(d) that it will promptly notify the data exporter about:

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- (ii) any accidental or unauthorised access; and
- (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

5(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

5(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

5(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

5(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

5(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

5(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6. Liability

6(1) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6(2) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6(3) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7. Mediation and jurisdiction

7(1) The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

(b) to refer the dispute to the courts in the UK courts.

7(2) The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8. Cooperation with supervisory authorities

8(1) The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

8(2) The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8(3) The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data

importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9. Governing law

The Clauses shall be governed by the law of the country within the United Kingdom in which the data exporter is established.

Clause 10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 of the Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11. Sub-processing

11(1) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11(2) The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11(3) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the United Kingdom in which the data exporter is established.

11(4) The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12. Obligation after termination

12(1) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12(2) The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

This Appendix 1 shall be deemed completed with the information set out in Schedule 1 to the underlying Agreement as applicable.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Mirion Technologies Cybersecurity and Data Protection Program

as of 13 September 2021

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.
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.
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.