Date	Name	Role	Change	Version
Wed Aug 06 2025	Tim Murnaghan	CTO	Approved	V1.0

Third-Party Risk Management Policy

General

This is the baseline practice for the identification of risks related to suppliers and other third parties, including cloud providers, having access to Integrum ESG facilities, networks, systems, and information assets. Identifying the risks from third-party access will help to ensure the security of Integrum ESG's information assets, equipment, and facilities.

Purpose and Scope

This procedure defines Integrum ESG's Third-party Risk Assessment and management process.

Terms and Conditions

Third party: Any persons or entities that are not Integrum ESG employees and are providing any services or engaged in a contract with Integrum ESG.

DPA: (Data Processing Agreement) – a legally binding document signed between two key data processing actors under GDPR – the controller and the processor.

Personal data: means any data that can or may be used whether alone or in combination with other information to identify a single person. Accordingly, Personal Data could include:

- Data that directly identifies an individual (such as their name, contact details, credit card details, geographical location); and
- Data that can be combined with other information to identify an individual or single out an individual (such as IP address, device ID, online identifiers, etc.).

General Requirements

All business arrangements with external parties shall be protected with a Non-Disclosure Agreement (NDA) that is signed and approved by both parties, and a formal contract, as applicable. An NDA may not be signed in cases where we accept the third party's terms and conditions as enough. Example after reviewing the SOC2 report of the third party. The contract shall define the following:

- Required access level to the information of the Company
- Provided IT-related products

- Services provided by the third party
- Agreements related to intellectual property.

The contract shall contain all security and privacy requirements relevant to the interaction between the Company and the third-party service provider. This shall include:

- Non-disclosure of the Company's information (Integrum ESG)
- Authentication Type
- Duties
- Security Controls to cover Privacy, Confidentiality, Integrity and Availability (CIA) of the information
- Auditing, logging and monitoring processes
- Backup and recovery of Company data
- Incident management (detection and reporting to the Company)

When relevant, the contract shall also cover the following issue:

- Attention being paid to the risk of possible conflicts of interests, or information leakage resulting from parallel contracts with the Company's competitors.

Method

If there is a business requirement to grant a third party logical or physical access to Integrum ESG facilities, networks, systems, or information assets, a business case must be created by the Integrum ESG business owner to identify the risks from the third-party access. The business case must include a risk assessment to identify any requirements for specific security controls.

The risk assessment must include:

- The type of access required.
- The sensitivity and criticality of the information at risk/exposure.
- The access controls are employed by the third party.

- The potential risks of this access to the confidentiality, integrity, and availability of Integrum ESG's information based upon a risk analysis of threats, vulnerabilities, and existing safeguards and countermeasures.
    - **Confidentiality**: The protection of sensitive information from unauthorized access.
    - **Integrity**: The assurance of the accuracy and reliability of data and systems.
    - **Availability**: Ensuring that information and systems are available and accessible when needed.

Each vendor will be assessed on a scale of 1 to 3 for each CIA principle, where:

- 1: Low risk
- 2: Moderate risk
- 3: High risk

The sum of the scores will be calculated for each vendor. If the total score is deemed as high (total score exceeding a defined threshold), the SOC 2 report of the vendor will be reviewed. If a SOC2 report is not available, the vendor will then need to complete a security questionnaire.

Regardless of the score, if a vendor is deemed critical (e.g., handling sensitive data), the SOC2 report will be reviewed and the DPA in order to verify that the vendor will notify Integrum ESG should there be a security incident.. Vendors handling sensitive information or providing critical services will be designated as "critical vendors."

Approval

All business cases for third-party access must be approved by Integrum ESG's CISO and the VP R&D before such access can be granted. The business owner must ensure that the business case is approved prior to contracts being signed. Such access could be network access for software maintenance or support, or physical access for various reasons.

The Third-Party Contract

General: Legal and Information Security, in accordance with this procedure, shall review contracts related to sensitive data exposure risks. All agreements or contracts with third parties that store Integrum ESG information must grant the company the right to review relevant third-party systems and networks or contain a commitment

from the third party to submit to independent periodic reviews and to release the results of those reviews to Integrum ESG. These agreements or contracts must include terms obligating the third party to adhere to Integrum ESG security policies. When Personal Data is involved, the third party must sign a DPA.

All related security terms should be included in a security appendix added to the third party's contract. Such an appendix should include requirements for data confidentiality, integrity, and availability controls, explicitly defined.

Controls must cover all appropriate physical, personnel, and logical information protection risks and must be consistent with prevailing statutory and regulatory requirements. When relevant, the DPA could be included in such an appendix, be part of it, or substitute it.

The information security appendix: The mentioned security appendix must include a statement about safeguarding Integrum ESG's Intellectual Property rights and copyright assignment and protection of any collaborative work. It should also materially include the following related principles:

- Maintain recognized industry practice safeguards and Integrum ESG standards and practices against the destruction, degradation, loss, unauthorized disclosure, or alteration of Integrum ESG Intellectual Property, assets, data, or any component Integrum ESG information systems, while in the possession or under the management of the third party. Safeguards shall be no less rigorous than the Integrum ESG security policies and procedures.
- Ensure that Integrum ESG data, Intellectual Property and third-party software under third party's care are properly managed by using recognized industry practices and Integrum ESG standards and practices for configuration management, document control, backups, etc.
- The Third-Party should have institute industry-recognized practices and system security measures.
- Whenever any Integrum ESG data is lost or damaged, the third party must use all commercially reasonable efforts to assist Integrum ESG in replacing or regenerating such lost or damaged data without additional charge or expense to Integrum ESG.
- The mentioned security appendix must include a clause clarifying that the third-party vendor must immediately notify Integrum ESG when a security incident related to Integrum ESG data has occurred or when a related suspicion has arisen. Integrum ESG on its part will decide what kind of respective action should be taken.

Terminating Third Party Contracts: Upon termination of any contract between Integrum ESG and a third-party organization handling Integrum ESG information, the third-party organization must immediately, if permitted by laws and regulations, to destroy or return all the Integrum ESG data or Integrum ESG property in its possession, irrespective of the party who initiates the termination.

Acceptable Use: Integrum ESG resources must be used only for business purposes by the third party. All third-party personnel must comply with acceptable use policies and not engage in any activities that are outside their

scope of responsibilities. This would include any unauthorized penetration testing, network or system scanning or monitoring, etc.

Integrum ESG reserves the right to conduct an investigation and, if necessary, revoke access privileges if a third party does not comply with Integrum ESG ’s acceptable use policies. If a security investigation is conducted, the third party must hand over any property requested as part of the investigation by Integrum ESG Information Security.

Related Security Controls: To ensure security compliance of the third party, the following security controls should be implemented.

- Verification that the NDA is signed by the third party.
- Verification that the vendor’s Security standard was reviewed and approved.
- Review and approve of the security statement.

The control process: The security relationship with a third party needs a dedicated control process, mainly related to the security appendix. Such a process will consist of the following tasks and responsibilities.

- Adapting the security appendix to the service provided by the third-party: CISO
- Review and approval of the security appendix: CISO
- Verification that the DPA or NDA is signed by the third party: CISO.

Re-evaluation Process for Vendors

All vendors, regardless of their initial risk classification, will undergo annual re-evaluations to ensure the continued appropriateness of their access to Integrum ESG systems, and information assets. Critical vendor's SOC2 reports will also be reviewed on an annual basis.

Re-evaluations may be triggered by significant changes in the vendor's operations, services provided, or any other factors that could impact the risk profile.

Security incidents involving the vendor, changes in regulatory requirements, or other relevant events may also trigger a re-evaluation.

The results of the re-evaluation, including any changes to the risk classification, will be documented and maintained in the Integrum ESG Asset Register.

Updated risk assessments and classifications will be communicated to the relevant business owners and stakeholders.

Privacy Requirements from Third Parties

Integrum ESG selects only suppliers that can provide technical, physical and organizational security that meet Integrum ESG's requirements in terms of all the personal data they will process on Integrum ESG's behalf.

- The Quality team have in place appropriate checks to ensure that all contracts are annually reviewed to determine if personal data is processed. These checks are carried out even when data processing activities are not the primary reason for the contract.
- Integrum ESG's third parties should not engage another processor without prior specific or general written authorization of Integrum ESG. In the case of general written authorization, the third party shall inform Integrum ESG of any intended changes concerning the addition or replacement of other processors, thereby giving Integrum ESG the opportunity to object to such changes.

Suppliers from outside the EU, processing personal data, will only be selected under the following conditions, in addition to the conditions described elsewhere in this document:

- If the supplier or the state in which it resides has been positively identified in an adequacy decision by the EU Commission
- OR
- When legally binding corporate rules exist, and organizational and technical safeguards have been established between Integrum ESG and the supplier to secure the rights and freedoms of data subjects that are at least equal to those afforded within the EU.
- OR
- When the arrangement has been approved by the supervisory authority.

An information security risk assessment, considering the information security controls of ISO 27001 Annex A, is carried out before a supplier is engaged. Supplier risk assessments are conducted by the CISO in accordance with the Integrum ESG.

If the Data Protection Officer considers it necessary, because of the nature of the personal data to be processed or because of the specific circumstances of the processing, an audit of the supplier's security arrangements against the requirements of ISO 27001 will be conducted before entering into the contract. Integrum ESG requires a written agreement that the service will be provided as specified and requires the supplier to provide appropriate security for the personal data it will process. All data processing contracts should allow Integrum ESG to conduct regular audits of the supplier's security and privacy arrangements during the period in which the supplier has access to the personal data. All data processing contracts should forbid suppliers from using subcontractors without Integrum ESG's written authorization for the processing of personal data.

- In the event that Integrum ESG permits a supplier to subcontract processing of personal data, the immediate supplier must prohibit the second-level contractor (or for lower level contractors) from subcontracting these processing operations without Integrum ESG's written authorization.

Contracts with second-level subcontractors will only be approved if they require those subcontractors to comply with at least the same security and other provisions as the primary subcontracting supplier. In addition, they are required to specify that, when the contract is terminated, related personal data will either be destroyed or returned to Integrum ESG. This applies to all successive levels of subcontractors.

Hiring External Employees/Contractors

General Requirements

Strict implementation of the need-to-know principle relating to the Company's information shall be applied whenever hiring external employees, temporary employees, contractors, consultants and interns.

External employees shall always sign an NDA before beginning working for the Company.

External employees must be trained on Cyber Security and GDPR if applicable prior being granted any access rights to Integrum ESG systems and platforms.

The HR Manager shall be responsible for defining and implementing the relevant policies for performing screening and background checks when hiring external employees.

Upon termination of their work, external employees shall submit all information related to the Company that was received and/or created during their work to their direct Manager.

The Company representative appointed by the CISO shall verify that all information and security system authorizations for the external employees are revoked immediately after the termination of their work.

The HR Department shall verify that all equipment assigned to the external employee is returned to the Company before the employee leaves. For additional information, *HR Policy*.

Access Control Policy for Third Parties

General Requirements

The Company shall develop and implement processes for ensuring adequate authorization to the Company assets for all third parties. When authorizing access to third parties, the access control shall be based on business requirements, while applying the following basic security principles:

- Least privileges
- Need-to-know

Local Access

Local access shall only be provided when the relevant business unit owner or direct manager determines that these privileges have a legitimate business need for such access, and after the approval of the CISO.

If approved, the local access mechanisms shall be based on the Company-acceptable security guidelines.

Remote Access

Remote access privileges shall only be provided when the relevant Company business unit owner or direct manager determines that there is a legitimate business need for such access, and after the approval of the CISO. Remote access for third parties shall be as limited as possible.

The criticality of the data/system shall be determined prior to the approval of any remote connections. If approved, remote access mechanisms shall provide the greatest level of security and prevent unauthorized users from gaining access to non-required Company assets.

- Public (Unclassified) information does not need to be labeled.

Responsibilities

Responsibility to follow this policy applies to all Integrum ESG employees. The CISO is responsible for developing, maintaining, and implementing the Third Party Risk Management Policy.

The roles and responsibilities of the respective employees at Integrum ESG are set out in the Roles and Responsibility Policy.

Document Ownership

The Policy Owner is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with Integrum ESG’s review requirements. A current version of this document is available to all members of staff in the company Shared Drive, Folder, etc.