Version 1.0 - September 2020

Information Security Policy

CONTENTS

1 INTRODUCTION

This Information Security Policy presents the general objectives Indaver wants to achieve in terms of information security. This policy concerns Indaver's information security domains including general data security topics (GDPR) and cybersecurity (incl. phishing, ransomware etc.).

Indaver ensures that its information security complies with legal requirements and meets its stakeholders expectations.

Indaver's information security is pragmatic and targets real and concrete needs based on risks and security maturity assessments.

Scope

This Information Security Policy governs the security of Indaver's systems, devices, applications and information deployed in support of our business activities.

This policy is available to all those working for or on behalf of Indaver and made available on the Indaver website to Indaver's suppliers, customers and stakeholders.

Governance – Roles

Indaver identifies different roles to establish and safeguard its information security. These roles are taken by different experts within the company.

Information Risk Owner (Executive level)

The Senior Information Risk Owner (SIRO) is accountable for information risks within Indaver and advises the Board on the effectiveness of information risk management across the organization. This role is taken by Indaver's Chief Information Officer (CIO). Operational responsibility for Information Security shall be delegated by the SIRO to the Indaver Information Security Responsible.

All Information Security risks shall be managed in accordance with the Indaver risk management Procedures.

Information Security Responsible (Business/process level)

The Information Security Responsible is responsible for the the day to day operational effectiveness on a business and process level of the Information Security Policy and its associated processes. This role is taken by Indaver's ICT Operations Manager.

Business Support Responsibles (Operations level)

The Busines Support Responsibles are responsible for the day to day operational effectiveness of the Information Security Policy and its associated processes. This role is taken by Indaver's BIS (Business Information Services) Managers.

Data Protection Responsible

The Data Protection Responsible is responsible for ensuring that Indaver and its Privacy Policy, constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. This role is taken by Indaver's Manager Legal & Insurance.

All Staff

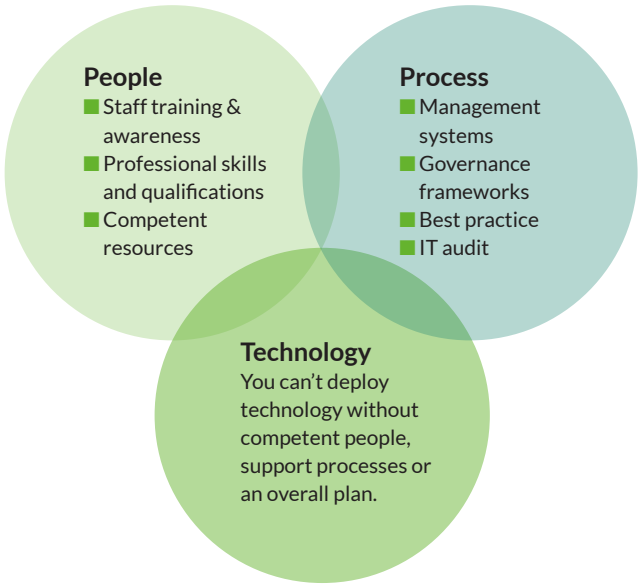
Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Indaver business.

2 OUR STRATEGY

Indaver's Information Security Strategy is based on 3 key assets: People, Process and Technology (PPT). As standalone components, people, process, and technology are necessary for conducting business. To achieve a high-quality, standardized and compliant information security in all three domains, balance and good relationship among those components is crucial.

People, process and technology in balance

As a term, PPT refers to the methodology in which the balance of people, process, and technology drives action: People perform a specific type of work for an organization using processes (and often, technology) to streamline and improve these processes. This framework supports Indaver in achieving a high level of information technology management.



People

When dealing with information security, it is our aim to create awareness about the behaviour of our employees in this domain. We are providing all necessary tools to train and acquire the required skills in order to understand how to protect ourselves as a company and the information we manage for and from our stakeholders and how cyber attacks are taking place.

Process

Here we establish mechanisms to achieve information security program objectives and monitor our performance.

Technology

With Technology we refer to the products and solutions required to protect our systems and data.

Standardized information security management system

Driven by one of our core values 'continuously improving' it is Indaver's ambition to eventually have its efforts regarding information security be aligned with the best practices of the ISO/IEC 27001 certificate. This way Indaver manages the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties in the best possible way.

3 CYBERSECURITY

NIST Cybersecurity Framework as a basis

As a waste management company Indaver must balance a rapidly evolving cyber threat landscape against the need to fulfill business requirements. To manage the risks, Indaver follows the **NIST Cybersecurity Framework Version 1.1.** This Framework provides a common language for understanding, managing and expressing cybersecurity risk to internal and external stakeholders.

Image source: The U.S. Commerce Department's National Institute of Standards and Technology (NIST) version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework, https://www.nist.gov Credit: N. Hanacek/NIST

This framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures. The Framework also helps to respond and recover from cybersecurity incidents, to analyze root causes and how to make improvements.

How Indaver coordinates the Framework implementation

Indaver shares its information and decisions at the following levels within its organization:

- *Executive*
- *Business/Process*
- *Implementation/Operations*

Indaver adopted the NIST Framework and customized it into its own 'Profile'. This means that we established a roadmap for reducing cybersecurity risk that is well aligned with our organizational goals, considers legal/regulatory requirements and industry best practices and reflects risk management priorities.

A circular flow

At Indaver, this is translated into a circular flow illustrating a continuous process in

which communication is guaranteed through different organization levels in a top-down and bottom-up flow. We believe that this circularity is key in achieving the best results.

Top-down implementation

It is the executive level that communicates the mission priorities, creates the available resources and overlooks the overall risk tolerance to the business/process level.

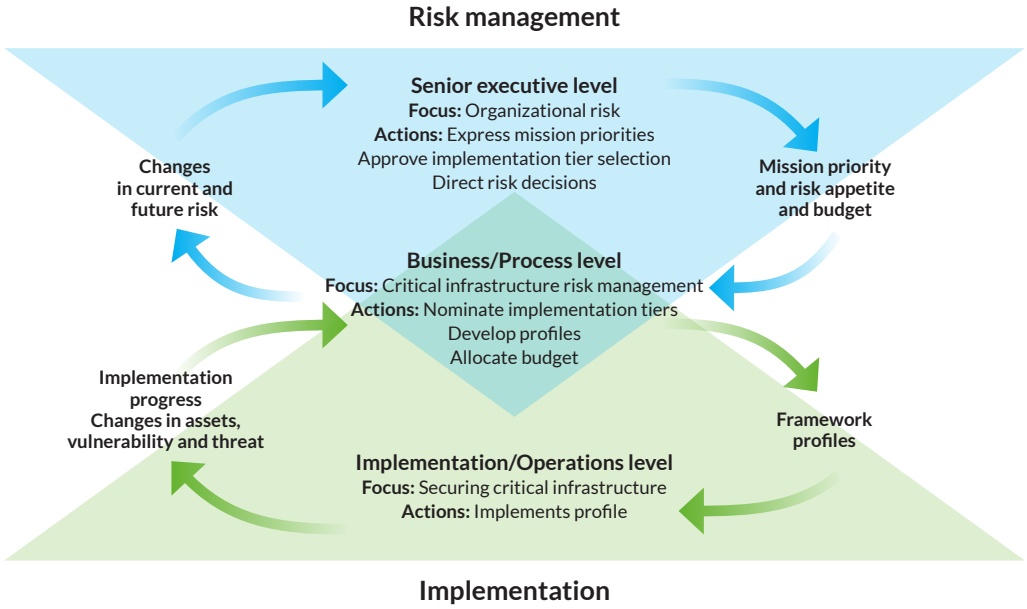
The business/process level uses the information communicated by the executive level as input and guidelines to implement and control the risk management process. In doing so, they collaborate with the implementation/operations level. This way, the latter are also informed and aware of the Indaver 'profile' business needs at any moment and can act accordingly.

Bottom-up implementation

The implementation/operations level communicates the implementation progress to the business/process level. At their turn, the business/process level uses this information to perform an impact assessment. The business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

This is how Indaver guarantees that there is awareness of cybersecurity risk at all organizational levels in order to secure its operations and activities. There is an organization-wide approach to security risk management with risk informed decision-making, policies, procedures, and processes. This way Indaver is cyber-resilient.

Notional information and decision flows applied within Indaver



Cybersecurity lifecycle is leading

Our cybersecurity strategy takes into account the entire cybersecurity lifecycle.

The cybersecurity lifecycle

Anticipate & Identify | Protect | Detect | Respond | Recover

This means that, together we renowned partners, we analyse every stage of the cybersecurity lifecycle. We first identify our critical assets and data, prepare our security strategy and ensure it is working. The next step is to deploy the right technology to defend our organisation and monitoring it against cyber threats. After that, we collect information from monitored elements, correlate them and detect breaches. Being able to qualify, contain and remediate attacks is and remains a priority. We stay on the lookout for the latest threats, hunt for leaks and fraud.

How we mitigate cybersecurity

When we apply this lifecycle on Indaver as a waste management company, we have taken all measures in all 5 of the domains of the cybersecurity lifecycle.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Anticipate & Identify

The activities in the Anticipate & Identify domain are foundational for effective use of the NIST and PPT Frameworks we mentioned earlier. In this domain, Indaver oriented itself supported by its shareholder and by external parties to have a good understanding to manage cybersecurity risk to systems, people, assets, data and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables Indaver to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of this outcome categories within this function include both best practices like Security Maturity Assessments, ITSM* based on ITIL** and risk assessments such as eg. ethical hacking and vulnerability management.

** IT Service Management*

*** Information Technology Infrastructure Library*

More concretely, we refer here to identifying the risks and taking actions. That is why Indaver conduct risk assessments on a structural basis, making sure there is inhouse and sourced technical expertise and up-to-date knowledge in these matters and clear governance of roles and responsibilities (see previous chapters).

Protect

In the second domain 'Protect', Indaver has developed and implemented appropriate safeguards to ensure delivery of critical services.

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. At Indaver this includes: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance and having Protective Technology implemented.

More concretely, we refer here to installing NextGen (web application) firewalls, SSL VPN appliance, e-mail security, endpoint protection, Identity & Access Management with strong password policy and Multi Factor Authentication (MFA).

Additionally we create awareness through factsheets, announcements on intranet and our personnel magazine and e-learnings to make our employees aware.

Detect

In the following domain 'Detect', we continuously develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events by AI-supported detection of anomalies and suspicious patterns. Examples include: Anomalies and Events; Security Continuous Monitoring and Detection Processes.

Respond

To comply with the fourth domain 'Respond', Indaver continuously develops and implements appropriate activities to take action regarding a detected cybersecurity incident. We have established a CSRT (cyber security respons team) and can rely on third party specialist for mitigation. We have a response planning, set up communications and can conduct an analysis for improvements.

Recover

In case of an incident, Indaver is able to recover in function of specific scenarios and back-up activities. Indaver has appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This supports us to timely recovery to normal operations and to reduce the impact from a cybersecurity incident. Also here we rely on our incident recovery plan and back-up assets.

4 COMPLIANCE REQUIREMENTS

Legislation

Indaver is obliged to abide by all relevant national and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Indaver, who may be held personally accountable for any breaches of information security for which they may be held responsible. Indaver shall comply with all relevant legislation appropriate; this includes but is not limited to:

- *Data Protection Act 1998*
- *Freedom of Information Act 2000*
- *Computer Misuse Act 1990*

Control

A regular auditing of this policy is required. This will be performed by a dedicated team and controlled by the Information Security Responsible.

Additionnally, an annual (financial) audit is performed by a specialised auditor and other assessments are done by different independent third parties. During these audits, these parties also control and take into account the level of (information) security of Indaver's operations and activities. It is in Indaver's interest and that of its stakeholders to continuously invest in its information security and it is supported and evaluated on an annual basis by its Board of Directors.

Review & continuous improvement

This policy shall be reviewed at least annually. The Information Security Responsible shall be responsible for ensuring the review is conducted in good order and follows due process for approval. Indaver's cyber security and confidential information loss prevention program is continuously improved:

- *Outside experts conducted independent assessments, including penetration tests.*
- *Indaver has a quality management program (ISO9001) for all its activities.*
- *Training on information systems security policies and best practices is completed for all information systems professionals.*
- *End-user security training remains mandatory for all employees. Cybersecurity tips are published regularly to increase employee awareness.*
- *New fraud management tools have been implemented to identify and preempt fraud attempts.*

Contact

If you would have any questions or concerns regarding this policy or Indaver's information security activities, please contact Indaver's Business Information Service/Security department via **cybersecurity@indaver.com**.