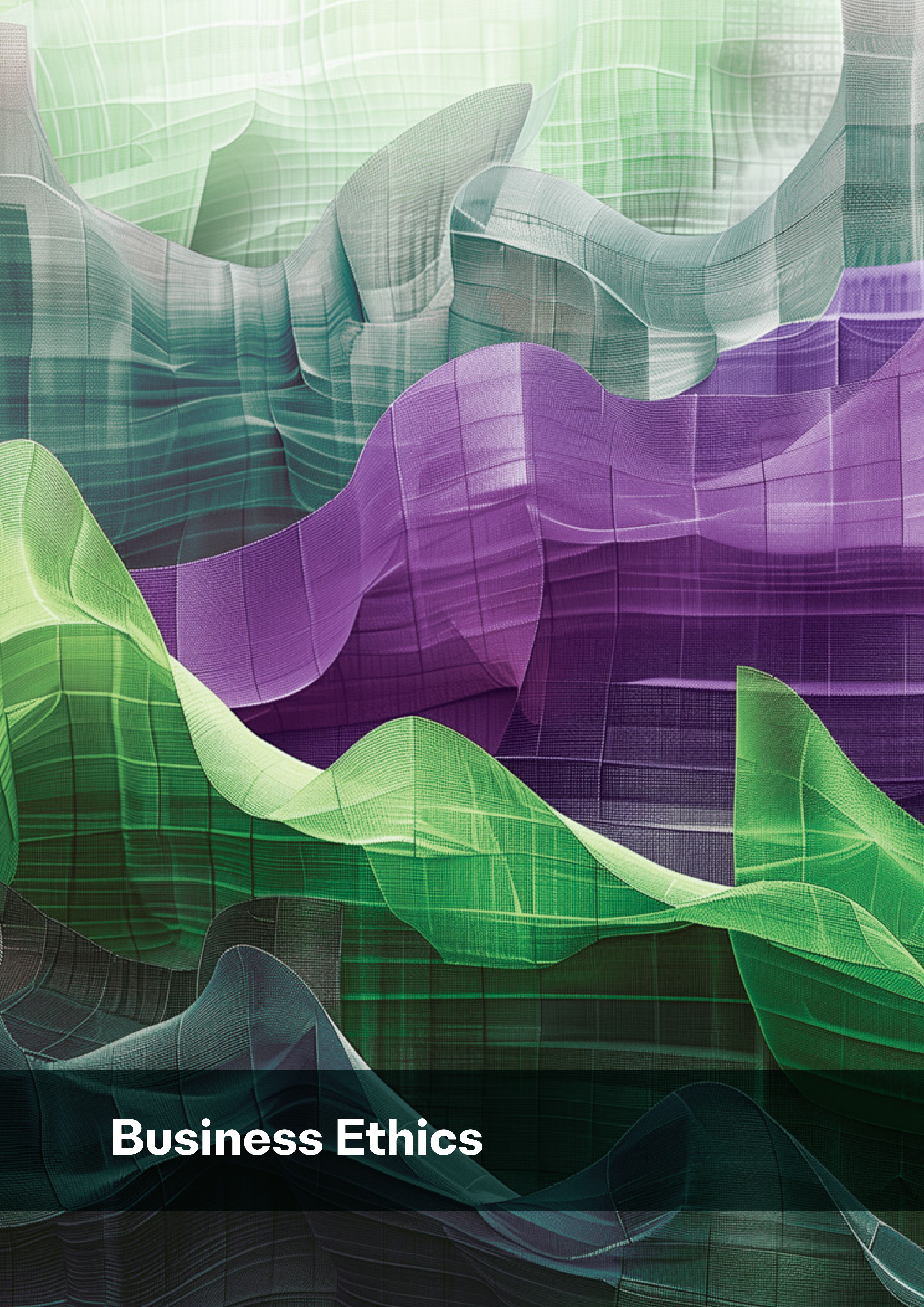
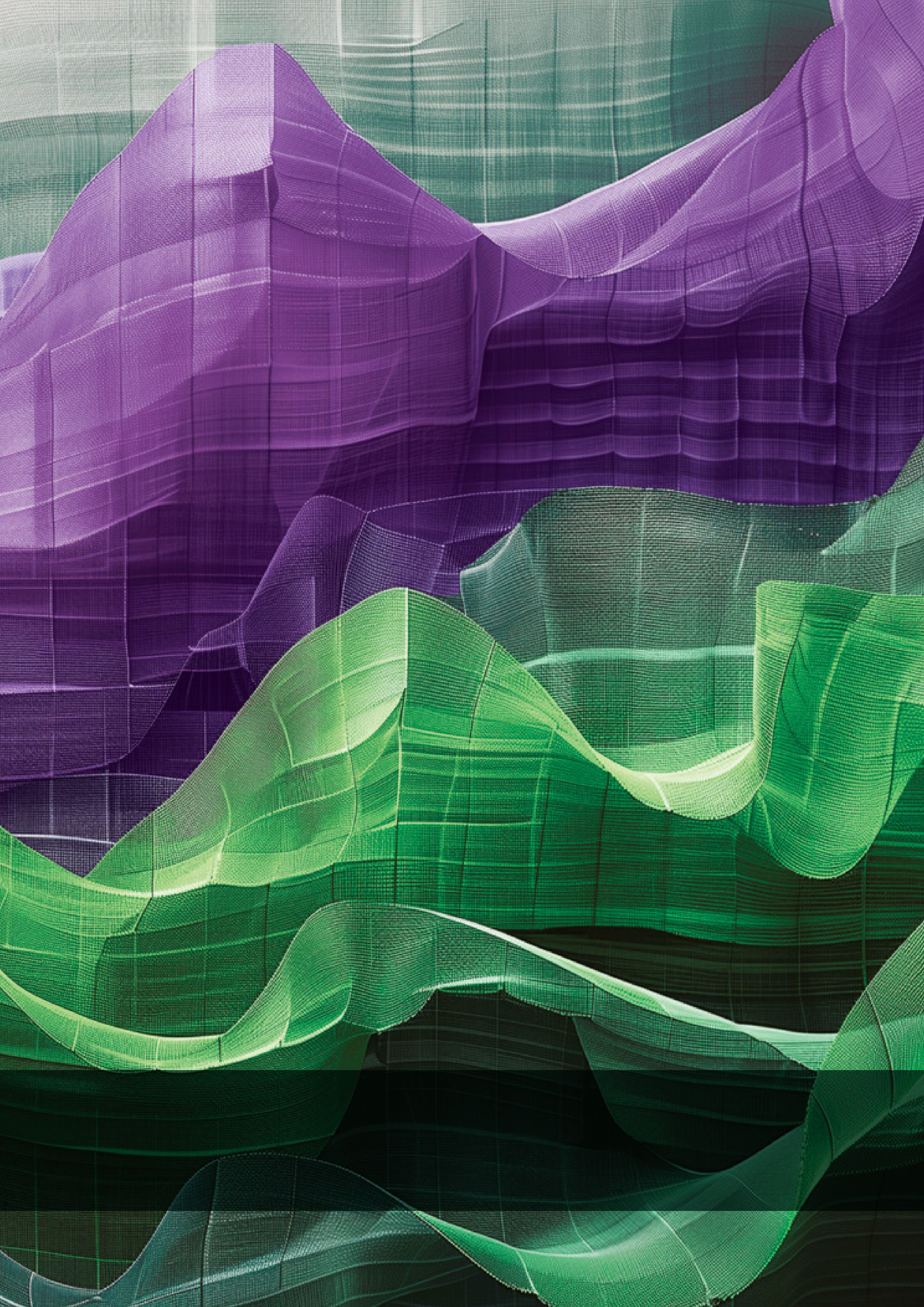


Business Ethics



We believe in an ethical approach to business, in a set of behaviours and values that determine an individual's conduct within and towards the community

The creation of value in the medium- and long-term and the achievement of strategic objectives will not happen without adopting, promoting and guaranteeing an ethical approach to business, which at Sisal is based on three pillars: **Business Integrity**, **Data Ethics**, **Security**. It is a commitment that translates into the fight against bribery and money laundering, the protection of privacy and corporate assets, and cybersecurity, with a growing focus also on respect for human rights and non-discrimination. We are committed to this approach along the entire chain and in all the countries where we operate.

Our ethical framework

First company in the gaming sector in Italy to obtain the

ISO 37001:2016 certification

of the Anti-Bribery Management System

(page 160)

Activation of

Speak Up! platform

for receiving and managing whistleblowing reports, available in all the Group's languages

(page 162)

Implemented and certified an

Information Privacy Management System (ISO 27701: 2019)

(page 164)

Sisal now has a

Chief Information Security Officer (CISO)

for infrastructure and IT systems security

(page 165)

Our objectives

8 DECENT WORK AND ECONOMIC GROWTH 16 PEACE, JUSTICE AND STRONG INSTITUTIONS	Target value	Year	Progress in 2023	
% hours of ICT system availability to support the gaming platforms*	100%	Every year	**100%**	◎
% employees attending training activities on business ethics, data privacy and security**	≥95%	Every year	**97%**	◎

* Calculated as the average availability of the various businesses and services

** All employees are required to complete courses on business ethics and data privacy within a set period after their date of hire.

◎ Target achieved → Progress in line with target ⊕ New Target

Our impact

Business Integrity

The ways Sisal and its employees act, in compliance with the law and regulations and inspired by the principles of legality, loyalty, fairness, transparency and responsibility.

(page 160)

Data Ethics

The adoption of fair and honest practices for collecting and processing personal data (in terms of methods, types and purposes) and insistence on maximum transparency towards our customers.

(page 163)

Security

Respect for the confidentiality, integrity and availability of IT infrastructure and systems

(page 165)

Business Integrity

The ways Sisal and its employees act, in compliance with the law and regulations and inspired by the principles of legality, loyalty, fairness, transparency and responsibility.

Combating Bribery

Sisal Group is committed to preventing and combating the commission of offences in the conduct of its business, in full compliance with the provisions of law, regulations, and all requirements under international standards and guidelines. In this context, **bribery is an intolerable obstacle**. We therefore have a responsibility to actively contribute to combating it with a **system of rules, models, controls and training and communication measures** constantly developed and promoted at all levels of the organisation.

All Sisal people are duty bound to comply with anti-bribery legislation. In particular, all the relevant documents are easily accessed via the website and intranet portal and all employees are also constantly involved in **training and communication initiatives,** especially those engaged in sensitive, at-risk activities.

Sisal is also the first company in the gaming industry in Italy to have obtained **ISO 37001:2016 certification (Anti-Bribery Management System)**, which is designed to mitigate risk relating to bribery (active or passive, attempted or committed, public or private).

Sisal employs **specific instruments** that have been upgraded (such as due diligence) to satisfy legal requirements (such as the Anti-Bribery Conformity function). All this testifies to and strengthens the **internal control system**, ensuring it is in a position to manage and limit the risk of "mismanagement", which not only causes economic harm, but also and more importantly, reputational damage.

Models and tools

- Adoption and diffusion of the Code of Ethics and Conduct, which expresses the principles of conduct to which all Sisal personnel and all stakeholders should adhere.
- Adoption and diffusion of the Bribery Prevention Policy, which defines Sisal's commitment to achieving anti-bribery objectives.
- Adoption of Model 231, which defines the set of rules and internal organisation procedures to prevent the commission of offences, including bribery.
- Strengthening of the internal control system with specific measures to prevent, combat and identify acts of external and internal corruption.
- Adoption of a Supervisory Board to ensure the suitability and implementation of the Organization, Management and Control Model.
- Creation of protected whistleblowing channels to use for any suspected corrupt act, whether attempted, certain or alleged, and adoption of rules that protect and guarantee the protection of whistleblowers.
- Creation of the Corruption Prevention Conformity Function, with the task of supervising and ensuring the implementation and operation of the anti-bribery management system.
- Training, information and communication of the measures implemented by Sisal and reporting tools.
- Provision of disciplinary measures targeting violations of the control system for preventing and combating bribery.

Conflict of interest management

Sisal has policies and procedures in place to **guarantee the communication, identification, management and monitoring of conflicts of interest**, whether potential or actual. Conflict of interest means any situation in which the expectations, interests or advantages of an individual employee are in conflict with the expectations, interests or advantages of Sisal, so affecting the individual's capacity to make decisions and carry out their tasks impartially and effectively. Sisal has therefore introduced an **Anti-Bribery Conformity Function (FCPC)**, which also monitors, records and manages conflicts of interest, as well as reporting any critical conflicts of interest identified to the CEO. Sisal also provides all subjects with whom it has relations of any kind[48], instructions for reporting any situation that could, even only potentially, generate a conflict of interest, mitigate an identified conflict and/or point out any shortcomings in the controls or management measures implemented.

Ethical and transparent commercial practices

Sisal is firmly committed to complying with all current legislation on competition and **promoting ethical and transparent commercial practices**. We strongly condemn any anti-competitive form of behaviour, including illegal agreements, abuses of a dominant position or any other practices that could jeopardise free competition in the market. We are well aware of the importance of healthy competition to foster innovation and ensure the quality of our products and services. To this end, we adopt strict internal policies and are committed to providing continuous training for our employees to **ensure full compliance with antitrust laws and protect fair competition**.

Respect for human rights and non-discrimination

Sisal has adopted a **Human Rights & Anti-Discrimination Policy** in line with major international agreements such as the Universal Declaration of Human Rights, the International Labour Organization's declaration on fundamental principles and rights at work and the principles of the UN Global Compact. Sisal's policy applies to all its employees, regardless of country and contract. We advocate the principles of diversity, equity and inclusion and the right to working conditions that respect the individual and their dignity, guaranteeing

- basic human rights, a minimum and fair salary, sustainable working hours and conditions, full access to workplaces and tools, exclusion of forced or underage labour (by checking age before hiring);
- the physical and psychological integrity and individuality of all persons;
- exclusion of all forms of behaviour entailing harassment or discrimination regarding gender, age, disability, nationality, sexual orientation, ethnic background, religion, political opinions and any other forms of individual diversity;
- freedom of expression, the right to participate in organisations that defend and advocate the interests of the individual, and the right to representation by trade unions or other bodies elected in compliance with current law and practice in the various countries where we operate.

To this end, we have special listening channels in place, from whistleblowing and grievance mechanisms to **periodical surveys** (DE&I, NPE, Culture), but we are aware that the absence of whistleblowing reports does not mean there are no potential problems and we therefore work proactively to anticipate specific needs and risk situations.

[48] This includes all members of the Board of Directors, the Board of Statutory Auditors and the Supervisory Board, employees of all levels and qualifications, on open-ended or fixed-term contracts, interns, temporary workers or similar, and third parties in general that have negotiating relationships with the company.

Whistleblowing

The management and a**ll Sisal employees are encouraged and required to report** any behaviours, including omissions, that are or might infringe laws and regulations or the values and principles set out in Sisal's Code of Ethics and Conduct, Model 231 and company policies and procedures, including behaviours associated with **internal fraud, mistreatment of employees** (e.g. discrimination, mobbing, harassment, retaliation), **occupational health and safety irregularities, bribery, conflict of interest, falsification of documents, misuse of company assets** (e.g. illicit use of company assets or information) or **breaches of privacy, IT security**, fiscal integrity of the organisation, etc. **All Sisal personnel receive specific training and regular updates** on what can be reported and through which channels. Employees and external subjects can also use **Speak Up!,** a whistleblowing platform available in all the languages spoken in the Group and managed by a third party organisation to ensure independence[49]. The whistleblowing channels are **always open and are managed by independent bodies** such as the **Supervisory Board (**formed by two external and one internal members of the Internal Audit department) and the **Whistleblowing Committee** responsible for receiving and processing reports (formed by the Internal Audit & Assurance Director and the Chief Risk & Compliance Officer). **Sisal accepts anonymous reports** and, whatever whistleblowing channel is used, **guarantees that the identities of the reporting and reported parties are protected and confidential** by processing their data in accordance with the law and taking all necessary measures. At the same time, Sisal forbids and punishes acts of retaliation or discrimination against the whistleblower for any reasons directly or indirectly connected with the whistleblowing. In 2022, Sisal received 37 reports, some of which related to alleged violations of the corporate code of ethics and internal procedures and policies, most of which were closed as unfounded.

Combating money laundering and the funding of terrorism

Ensuring effective and timely monitoring of the adequacy of its systems for preventing and combating illegal gaming, money laundering and funding of terrorism is a priority at Sisal. The **Group policy** defines the structure and organisation of the Group Anti-Money Laundering Function, as well as the general rules to which all Italian and foreign companies must adhere. The Policy is then articulated in **individual procedures and operating instructions** specific to the various separate entities, also with regard to national characteristics and requisites. In line with the **risk-based approach** and to fulfil the relevant legal obligations, Sisal carries out **monitoring using automated systems developed in-house on the basis of industry-specific know-how and databases provided by external providers.** Such systems make it possible, among other things, to carry out thorough **reputational screening** of players and retail network operating companies in order to verify **the existence of the legal reputational requisites**, both prior to contract stipulation and regularly thereafter. **Transaction monitoring, customer profiling** and documentation retention activities are carried out **using systems developed in-house and customised for the peculiar needs of the gaming world**. In particular, this enables us to monitor gaming operations for the purpose of identifying movements to flag and, where necessary, initiating the process of reporting the suspect transaction to the authorities. **Training is obligatory for all employees** (including new hires) **and collaborators** (including point-of-sale staff) to raise their awareness of the risks related to money laundering and the funding of terrorism. To step up the dissemination of knowledge in this area, **in 2023 a new training course for points-of-sale staff was developed and delivered**. The course centres on the main legal requisites relevant to the Company's core business operations and provides practical advice and examples of behaviours to adopt or avoid, especially in the context of verifying customers and reporting any suspect transactions.

[49] The platform is available at the following link: https://sisal.integrityline.com/frontpage. Reports can also be sent by post to the address: "Servizio Segnalazioni" Via Ugo Bassi, 6 - 20159 Milano.

Data Ethics

The adoption of fair and honest practices for collecting and processing personal data (in terms of methods, types and purposes) and insistence on maximum transparency towards our customers.

Sisal has adopted a series of **Data Ethics** principles to guarantee a decision-making process inspired by the highest values of business ethics.

- **Accountability:** Sisal has adopted a governance model to define and monitor control activities, and to strengthen the ethics, conformity and sustainability of services, which are always developed in compliance with requirements, using a "privacy by design and default" approach to guarantee personal data protection.
- **Ethics & Fairness:** Sisal adopts fair and equitable practices, with the objective of minimising discrimination and treatment that is penalising or biased.
- **Privacy:** Sisal processes customers' personal data in accordance with privacy principles and legislation and guarantees data minimisation, retention for limited periods, use for specific and transparent purposes and accessibility at any time.
- **Quality & Accuracy:** Sisal aims at a high level of data quality in terms of accuracy, precision and updating and adopts all the necessary measures to enable prompt rectification or deletion.
- **Transparency:** Sisal guarantees a high level of transparency clarity regarding the procedures, types and purposes of personal data collection and processing on channels, products and services provided to customers.
- **Responsible Data Sharing:** Sisal guarantees the adoption of technical and organisational measures needed to ensure legal compliance and also protect personal data processed by third parties acting in the name and on behalf of Sisal.

Data ethics control

In line with its declared Data Ethics principles, Sisal has adopted specific controls based on three main lines of action

1. Eminence & Strategy

- **Awareness and training:** special activities are organised at least annually to heighten the awareness of employees and third parties around data protection issues, implement a diffuse compliance model and guarantee correct management of business processes in terms of Privacy and Data Ethics.
- **Control framework:** continuous monitoring is carried out by means of second level controls on the aforementioned general principles (legality, transparency, correctness, minimisation and limitation of data retention, data controller accountability).
- **Transparency:** information notices and public documents are regularly prepared to illustrate Sisal's commitment and mission regarding Privacy and Data Ethics and management of data subjects' requests to exercise their rights.
- **Cookie management and compliance:** a process has been implemented for monitoring compliance with current law on cookies by Sisal's websites and mobile app.

2. Privacy & Accountability

- **Governance model:**
  Sisal has adopted an internal governance model to guarantee protection of personal data specific to business activities and identified the roles and responsibilities of subjects involved in ensuring that personal data are processed in compliance with applicable laws (first and foremost, EU Regulation 2016/679 (GDPR)), thereby improving the company's commitment and awareness in this area. A Data Protection Officer (DPO) has been appointed to provide consulting to the Data Controller and ensure that internal processes are aligned with current legislation. In 2023, Sisal also implemented and certified an **Information Privacy Management System according to ISO 27701: 2019** to support our commitment to continuous improvement.

- **Policy and procedures**
  To guarantee compliance with the relevant provisions of Privacy & Data Ethics law, policy and procedure documents have been drawn up and are regularly updated.

- **Processing Register**
  A process has been implemented to manage, monitor and update the processing register in order to guarantee tracking of Sisal's activities involving the personal data processed.

- **Exercising of data subjects' rights**
  A process has been defined for receiving and promptly responding to data subjects' requests to exercise their rights.

- **Privacy by design and by default**
  A checklist has been adopted to assess privacy protection "by design" and "by default" in the case of new initiatives, services or products.

- **Data Protection Impact Analysis**
  A risk analysis and impact assessment methodology has been adopted for types of processing that entail a high level of risk for data subjects' rights and freedoms, in line with the methods adopted by the company and with adequate security and prevention measures.

3. Responsible Data Sharing

- **Third-party contract management**
  To manage third parties involved in processing personal data, privacy clauses are drafted and negotiated in contracts and specific data protection agreements, and guarantees provided by the third party are verified.

- **Monitoring of third parties**
  Periodical audits are carried out on selected stakeholders that process personal data for Sisal, thus guaranteeing their observance of privacy and security requirements and therefore the correct processing of personal data along the entire chain.

- **Training**
  Regular training is organised for third parties, tailored according to the processes they manage on behalf of Sisal, so ensuring they know about the company processes and procedures to follow and the applicable legal requirements.

Security

Respect for the confidentiality, integrity and availability of IT infrastructure and systems.

Sisal sees **protection of its information assets and management of ICT and security risks** (including cyber risks) **as objectives of prime importance** to be pursued on a continuous improvement basis. **Cybersecurity** is an enabling factor in the pursuit of business objectives. This is why we have defined a specific **strategy** based on the following principles:

- guaranteeing **central security governance** designed to preserve the confidentiality, integrity and availability of the company's information assets;
- promoting the development and ongoing evolution of **security technology solutions** to ensure Sisal has a sustainable advantage in the long-term and in line with its objectives and values;
- favouring the construction of an adequate **organisational model for managing information security** and promoting development of the skills needed to keep effective protection systems in place;
- guaranteeing **compliance with applicable laws, regulations and standards** on information security, as well as with specific contractual agreements with various stakeholders;
- promoting **innovation in the field of security** to guarantee constant alignment with new technological developments and use of new generation methods, processes and solutions;
- guaranteeing **data security, resilience and protection** related to services offered to consumers, thereby increasing their reliability;
- spread a **culture of information security and sensitivity to cyber risks** in Sisal in order to raise the level of awareness about the behaviours involved and guidelines to follow to forestall threats;
- promoting adoption of a **risk-based approach** to implementing security measures by means of a framework built into the company's overall risk management model.

Security governance

Our cybersecurity strategy requires us to keep abreast of state-of-the-art security in our sector and aligned with changing risk scenarios. This is why we have a **Chief Information Security Officer** (CISO), who provides strategic vision and ensures ongoing improvement of processes to mitigate the cybersecurity risks we face. The CISO and their organisation work in synergy with Management, with the Business and Markets Areas, HR, Internal Auditing and Risk Management functions, and with the Compliance area. The main areas involved are:

- **Strengthening the organisational structure of the Security function**: in line with the organisation's growth and the expansion of the business into international markets, Sisal has scaled up the Security function and introduced new professional roles to upgrade the management of our security capability.
- **Security certifications**: Sisal implemented and maintains an Information Security Management System that incorporates the guidelines set out in the main industry standards and regulations, i.e. ISO27001 and WLA-SCS[50]. The compliance of our management systems is verified by periodical audits and checks by independent third parties.
- **Security Framework**: to define security requisites, adapt them for specific processes and verify their

[50] Certification issued by the World Lottery Association in compliance with specific gaming sector and international lottery standards. The perimeter includes Sisal Lottery Italia S.p.A, Sisal Loterie Maroc and Sisal Sans.

effectiveness, Sisal has developed and maintains a framework of policy, procedures and guidelines that it keeps constantly updated. It has first, second and third level controls and indicators for continuous monitoring.

- **IT & Cyber Risk management**: Sisal has defined an ICT and Cyber Risk management model that involves assessment and monitoring of the organisation's exposure to such risks and identification and implementation of risk mitigation measures.

Cybersecurity culture

Ensuring that people across the entire organisation are adequately informed on cyber risks and ways to reduce them is of vital importance in the pursuit of the company's business objectives:

- **Security Awareness**: Sisal regularly organises awareness sessions on various communication channels and tests their efficacy by simulating attack scenarios to verify the organisation's capacity to react effectively.

- **Security Training**: training activities are tailored to the various users' roles and provided at all levels of the organisation.

Security enforcement

Technological developments, digitisation of services, adoption of cloud services and the evolution of cyberattack scenarios are some of the phenomena that Sisal sees as drivers to strengthen its security posture. In 2023, initiatives were completed in the following areas:

- **Prevention**: we have invested in the upgrading of our cyber security capability by implementing new generation technological solutions. Priorities here were the access control system and identity management procedures, as well as protection measures for the devices employed by users to carry out their tasks. Data protection measures were also improved with encryption and anonymisation techniques, and vulnerability management technologies were strengthened, pursuing a risk-based approach. In addition, security testing activities are carried out on an ongoing basis, both as a routine part of software development cycles and on an impromptu basis on critical systems, and periodic internal and external audits are conducted at least annually. Lastly, Cyber Threat Intelligence practices were further improved to prevent, as far as possible, cyberattacks or events capable of negatively affecting the Sisal brand.

- **Detection & Response**: we have invested in security technologies to boost effectiveness in the security event and incident identification and response phases, strengthening both proactive and reactive protection measures. There was a special focus on gaming services and monitoring and alarm functions signalling anomalous events or behaviours were extended to enhance the capacity to promptly identify cyberattack or fraud attempts. Certain security technology functions already in place were extended to expand the monitoring perimeter and upgrade our critical event detection capability.

- **Resilience**: we have carried out periodic test activities to ensure that the operational continuity management system can effectively handle the main unavailability scenarios, also through penetration tests conducted with support from third parties.

Integrated management system

Sisal adopts an **Integrated Management System** to ensure continuous improvement of processes and services and the creation of value for employees, customers and stakeholders. This is the reason for ongoing engagement in the **certification process in the areas of Responsible Gaming, Quality, Customer Contact Centre Quality, Corruption Prevention, Information Security and Privacy, Occupational Health and Safety, Environment, Energy**.

For the purposes of promoting **customer centricity**, we also obtained the **ISO 182959001: 2017 part 1** Certification, assuring and continuously monitoring the contact center service provided to our employees and customers. We believe that customer satisfaction can be pursued through ongoing efforts to improve the quality of our processes and services. This involves an approach focused on risk-based thinking to identify possible **risk factors** and any opportunities for improvement, and a transparent and responsible dialogue with all stakeholders.

That's why activities are **periodically carried out to assess the risk profile** of the company's activities and processes and **monitor them using key performance and risk indicators (KPIs and KRIs)**, as well as internal audits to verify compliance with the requirements of the relevant ISO standards, from which action and improvement plans can emerge.

In addition, the independent certification body conducts annual audits to verify compliance and fitness to maintain the certificates obtained by the Company.

The findings of the activities carried out are brought to the attention of the Leadership Team during management reviews.

For Sisal, this is a commitment and a responsibility for the entire organisation: it's why we constantly sensitise all staff, at all levels and grades, to comply with the principles contained in the various Policies on the subject[51].

[51] For further details on Sisal's certifications and Policies, see the dedicated page at: https://www.sisal.com/eng/governance/certifications

Responsible supply chain management

We are committed to promoting our sustainability strategy along the entire chain.

Sustainability challenges are shared by everyone in the Sisal community, from suppliers to points of sale, so that medium-long term sustainability can be pursued.

The development of a **responsible and sustainable supply chain** is part of a broader corporate vision that values and actively protects social and environmental responsibility, fully integrating them into its strategy.

1,743
suppliers

Our suppliers

Our continued growth is made possible by building a **network of strategic partnerships with 1,743 suppliers**[52], carefully selected because they have the best specialist skills available on the market and are aligned with our values and objectives: **legality, business ethics, loyalty, fairness, transparency and meritocracy**.

The international development strategy has resulted in the **promotion of responsible purchasing** procedures, developed at Group level, also among purchasing teams in foreign countries, which are constantly supported by the **central Procurement function**, in order to supervise and support the acquisition of products and services.

A new Code of Conduct for third parties

Sisal has adopted a **Code of Conduct for third parties**, published on its website[53], which consolidates the principle that all public and private business initiatives must recognise, share and concretely apply the moral values and ethical principles that are the true foundation of any civil society.

Respect for human and employment rights, protection of the environment, prevention of corruption, security of information and privacy, and the promotion of responsible gaming, as well as legality, business ethics, loyalty, fairness, transparency and meritocracy, are the principles that guide the company's policies and procedures involving workers, suppliers, customers and third parties.

[52] The number of suppliers includes those in the Italian perimeter and its foreign subsidiaries
[53] The code is available to the public at this link.

In addition, the **International Procurement function** oversees all **negotiating activities** with foreign branch supply chains. These activities include scouting for new suppliers, preparation of tender documentation, assessment of offers, and selection and contracting of suppliers), and uploading contracts to the procurement platform.

Assessment and qualification process

Under our **Quality Management System**, we apply a stringent **assessment** and **qualification** process to suppliers that requires them to comply with current legislation in the gaming industry and with our stakeholders' expectations.

All our suppliers are required by contract to **comply** with the rules and principles set out in the **Code of Conduct for Sisal Third Parties**, including the obligation to operate in line with our ethical standards regarding employees' rights, environmental protection and workplace health and safety.

We have introduced **anti-bribery management** systems according to standard UNI ISO 37001:2016. Our procurement processes also take account of the characteristics that services, facilities and tools must have in order to ensure full accessibility, usability or adoption by everyone, in line with our commitment to the inclusion of people with disabilities[54].

In 2023, Sisal also began performing due diligence in relation to reputational and financial risks through the Moody's platform. This process is applied to all companies involved in negotiations for the supply of goods and services. Suppliers are assessed on the basis of their **compliance** with the provisions of contracts and orders, as well as by **monitoring** variance between the **service levels agreed** and those actually delivered and other factors such as delivery times, quality, costs and other contract specifications.

These controls are used for global supplier analysis and a twice-yearly updating of the **Vendor Rating Index (VRI)**, which records suppliers' overall performance and flags areas for improvement.

Sustainable Procurement

In 2023, Sisal began its reorganisation of the Vendor Management & Rating System for qualifying and monitoring its suppliers, making provision for the application of ESG criteria in both the supplier qualification and tender phases.
In detail, we have made plans to implement an ESGG[55] *Minimum Checklist* in the qualification phase of all suppliers with a significant impact on the business, and the implementation of a detailed *Environmental Checklist* in tender procedures, in order to identify suppliers with a strong commitment to environmental issues (e.g. suppliers that have set ambitious CO_2 equivalent emission reduction targets such as a Science Based Target[56]). The new system will be fully operational by the end of 2024.

In collaboration with the Procurement function, Sisal also launched a pilot project to implement a checklist of ESG requirements in the supplier selection process for some tenders in which purchases of goods or services had a significant impact in terms of indirect GHG emissions (e.g. logistics services, data centre, purchase of thermal paper).

[54] For more details, see our human rights and non-discrimination policy.
[55] ESG – Environmental, Social & Governance.
[56] Science Based Targets aim to reduce CO_2 and other climate-altering gas emissions in line with the Science Based Target initiative (SBTi), a partnership promoted by the UN Global Compact (UNGC), the World Resource Institute (WRI), the CDP (Carbon Disclosure Project) and the WWF, for which more than 2,000 companies worldwide have signed up.