Chapter 2

ORGANIZATIONAL ETHICS AND EXCELLENCE IN PERFORMANCE

Organizational Ethics

Bezeq's Code of Ethics

Bezeq's Approach to Ethics

Bezeq adheres to a business culture that is based on clear ethical rules. The Company ascribes supreme importance to fair and ethical conduct towards all its stakeholders, including its customers, employees, suppliers, competitors and shareholders. For us, this is the cardinal condition for value-based excellence and business leadership.

Maintaining business ethics is a managerial challenge and test of the highest order. Bezeq's management commits to lead the Company according to the standards set out in the Code of Ethics – Our Way of Doing Business, to serve as a model of personal integrity, fairness and probity, and to be a touchstone for any act or conduct on the personal, professional and organizational level.

Our Principles of Action

Excellence

Equality and fairness

Respect for others

Openness

Caring

Integrity

These are the principles that create the telecommunications experience we afford and that underlie Bezeq's Code of Ethics.

"Our Way of Doing Business"

Bezeq's Code of Ethics sets out principles and rules of proper conduct by which senior officers, managers and employees of the Company should guide their actions. The Code of Ethics, which was last revised in October 2018, was formulated in a comprehensive process that included collaboration by and workshops for the Company's managers and employees.

In terms of the nature and areas of activity of the Company, the code sets a "bar" – a practical ideal of what is right and proper, for which one should strive, and which is thus differentiated from rules and procedures that set a "threshold" – a mandatory minimum.

We at Bezeq believe that together we will continue to lead the Israeli telecommunications market in innovation and technological development. We will maintain a business culture that serves as a role model for other companies in Israel and will provide advanced services and novel technologies that enhance the telecommunications experience.

> **Ehud Mezuman, Vice President of Human Resources:**
>
> **"For us, there is no other way to do business.**
>
> The principles of action on which Bezeq's Code of Ethics is predicated, and the rules of conduct deriving from them, are the bar we set for ourselves in conducting our business, every day.
>
> Our Code of Ethics does not purport to answer every business situation we may encounter, but it does reflect a world view and foundation of values on the basis of which decisions should be weighed at any given moment in our business life. It is these decision-making junctures that present the greatest business challenge, namely – providing quality service, while at the same time keeping the environment clean and healthy."

From Bezeq's Code of Ethics:
"We treat ourselves and our fellow workers with respect, fairness and honesty. The differences that define us as individuals represent a human and business advantage for the group as a whole. Our vision is to attract the best people, to value and develop them, so that they contribute to our shared success."

Implementation of the Code of Ethics – Training and Instruction

The Code of Ethics is imparted in a special video that was produced for this purpose, as well as by frontal instruction (frontal sessions were held mainly in 2019, until the video was produced in 2020). A presentation was made to the Audit Committee in October 2019, showing the process of implementation in the organization.

In the fourth quarter of 2018, a refresher course was held on the subject of ethics, that was taken by **93%** of the Company's employees. In the last quarter of 2019, a video was distributed and a quiz was taken by **94%** of company employees.

Type of training / number of (employees (estimated	2018	2019
Refresher course on organizational knowledge management (digital (instruction	5000	5000
Refresher course for managers (digital instruction)	800	800
Managers' workshops in managerial courses	25	**75** ▲
Brief instruction sessions	180	180
Basic courses (digital instruction)	775	**899** ▲
Orientation days	50	50

Internal Auditing of Processes in the Company

In general, environmental and social issues are examined (in internal auditing processes), to ensure that the Company is complying with the regulatory requirements. The Company also has a Compliance Policy for the Prevention of Bribery and Corruption, and the internal auditor regularly promotes awareness of this issue. Some 9,000 hours of auditing were performed in 2019 by the Company's Internal Auditing Unit (most of them internally).

Risk Management

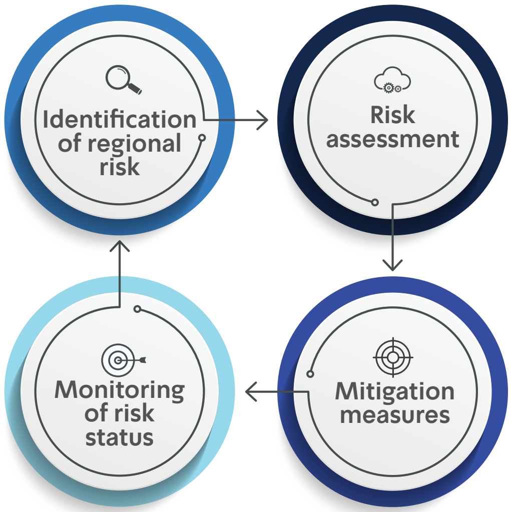
Risk management is a consistent, methodical, cyclical and continuous process, intended to improve the Company's ability to contend with risks. A risk is a potential event that, if it were to occur, may hinder the realization of the Company's business objectives.

Risk Management Procedure at the Company

The processes under Bezeq's risk management procedure are designed to instill the employees and managers with an awareness of the Company's comprehensive risk management culture. The procedure encourages correct decision making and contributes to the transparent handling of problems and incidents, including providing management and the board of directors with an up-to-date picture of the risks and the controls applied by the Company.

The procedure defines risk management processes for the Company as derived from the risk management policy that was approved by management, the Audit Committee and the board of directors. By means of this procedure the Company educates its employees safe and reliable risk management methods and makes these methods a part of its routine activity.

Risk management procedure:



Main Risk Management Plans at Bezeq

"Risk Appetite"

Risk appetite frameworks provide transparency and reflect constraints, serving as a point of reference for the management of risks and helping to prevent both excessive and overly conservative risk-taking. Risk appetite defines the extent of the effect (loss) Bezeq is prepared to sustain in assuming risks.

Key Risk Indicator – KRI

The KRI index is used for the dynamic examination of the risk status and intensity against the risk appetite that was defined in the risk map and in the mitigation plans, and the adjustment of the organization's activities to changes that have occurred.

ISO 27001

Bezeq implements a cyber security assessment process in accordance with ISO 27001. The assessment identifies risk factors that threaten the Company's information security, mapping out the inherent risk and the residual risk according to the activities and controls carried out by the Company. The purpose of the assessment is to protect the Company's information and improve the reliability, availability and integrity of its information infrastructures and databases. It is intended for all the Company's stakeholders, employees and customers.
Management is responsible for boosting employee awareness of existing information security risks and for acting to reduce the risk levels and set the residual risk at the lowest possible level.

Bezeq's Plan for Operational Continuity in an Emergency

The plan comprises:
Business Continuity Program (BCP)/Continuity of Operations (COOP)
Disaster Recovery Plan (DRP)

Business Continuity Program (BCP)

Business Continuity/Continuity of Operations is the component of the Emergency Management Doctrine dealing with the actions an organization must take to ensure that critical business functions are available to all the organization's stakeholders (customers, suppliers, regulators and other entities). The Business Continuity Program is meant to enable an organization to remain viable before, during and after an emergency. Bezeq achieves this by preparing in advance for various scenarios.

Apart from information technology, the program also addresses other aspects such as retention of key personnel, safety and security of installations, communications and goodwill protection. Bezeq also has a plan for crisis management and business impact analysis and it carries out process controls, on the basis of which coping strategies are formulated.

Disaster Recovery Plan (DRP)

Disaster Recovery involves a set of policies, processes and procedures to enable recovery from a disaster, such as earthquake, flood, missiles, building collapse, erroneous deletion, etc., that has shut down the technological infrastructure that is vital for an organization's activity. The Disaster Recovery Plan includes planning for the restoration of applications, data, hardware, communications and other elements of information technology, information, as well as cyber security procedures and a continuity plan for backup and survivability of the network and the infrastructure.

Plan stages:

1) **Mapping of risks -** an internal process that examines risks and analyzes their implications in normal conditions and in an emergency

2) **Definition of targets -** setting service and recovery targets based on a risk analysis

3) **Procedure -** manual of dedicated procedures for emergency scenarios

4) **Instruction and exercises -** instruction for the employees according to set procedures and implementation of an annual exercise plan for key processes

5) **Mitigation plans -** an ongoing process for the mitigation of risks and critical risk factors

6) **Control and update -** carrying out quarterly BCP status reviews and establishment of a steering committee to discuss cyber-related issues with management

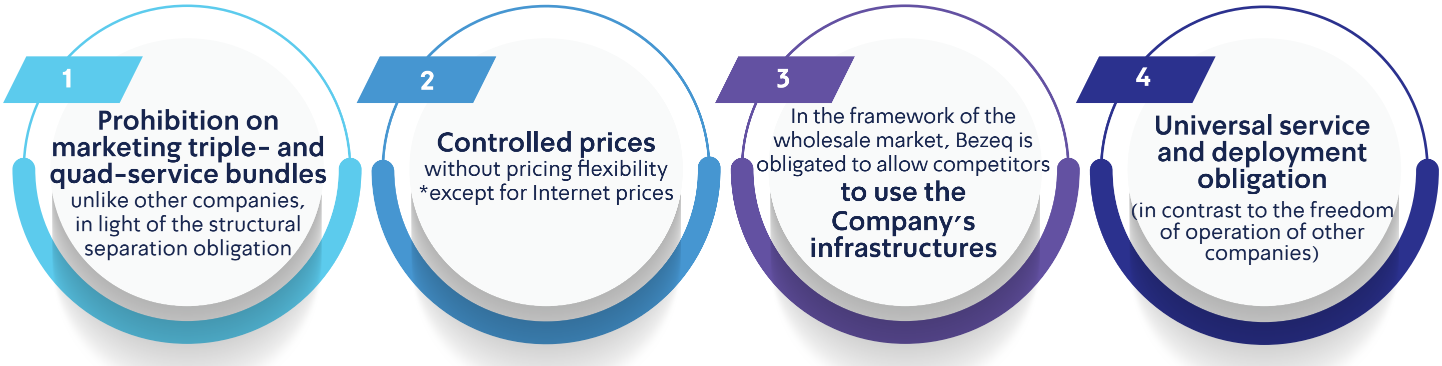
Marketing and Responsible Advertising

We welcome competition, as an ongoing challenge that brings out our best qualities - professionalism, creativity and innovativeness -in the best interests of our customers.

Bezeq as a matter of policy complies strictly with the antitrust laws and the communication laws, regularly enforcing them in all its divisions and departments and vis-à-vis all its managers and employees.

From Bezeq's Code of Ethics:

"Fairness and decency are our guiding principles in relation to products and services of our competitors. We strive for market leadership through the quality of our products and the service we provide, while observing the rules of fair competition... free competition gives real value to Israeli society, and we therefore strictly uphold/comply with state mechanisms that are intended to regulate and promote competition... Our activity as a business corporation rests on two foundations: the duty of trust and the duty of proper disclosure."



1
Prohibition on marketing triple- and quad-service bundles
unlike other companies, in light of the structural separation obligation

2
Controlled prices
without pricing flexibility
*except for Internet prices

3
In the framework of the wholesale market, Bezeq is obligated to allow competitors
to use the Company's infrastructures

4
Universal service and deployment obligation
(in contrast to the freedom of operation of other companies)

Bezeq's management has acted and will act at all times, conscientiously and with determination, to uphold and enforce these laws, fostering compliance, inter alia, through lectures, instruction programs and guidance booklets on the subject. **We do whatever is necessary to instill and refresh knowledge of the rules** – however, there is always room for improvement. Several fines were imposed on Bezeq in the reported year in connection with social/economic issues.

In **2018**, a financial sanction of NIS 250,000 was imposed by the Consumer Protection Authority in connection with an advertisement for cyber services.

In **2019**, the Anti-Trust Authority imposed a financial sanction of NIS 30 million for abuse of position (the process was initiated in 2018 in respect of events that occurred up to 2017 and is currently being appealed in the Anti-Trust Tribunal), as well as a financial sanction of NIS 4.2 million for failure to provide information (the amount was determined in 2020 in a settlement). Also in this year, the Ministry of Communications imposed a financial sanction of NIS 11.3 million for failure to supply wholesale telephony services, as well as a financial sanction of NIS 2 million in respect of the "reverse bundle" service.

Excellence In Performance

Bezeq's aspiration for excellence is self-evident both from its information and cyber security policy and from the safe environment it maintains for employees coupled with responsible supply chain management.

Information and cyber security

Bezeq complies with the civil market's strictest standards for information security. The Company considers the protection of its customers' information to be of paramount importance and takes responsibility for safeguarding customer information and enforcing the rules that protect privacy.

In today's world of ever-developing technology, challenges on the Internet have become more significant and substantial. Malware, viruses, phishing attacks and information theft are among the challenges of the new era. Safeguarding the privacy of our customers and securing their information is a core principle at Bezeq, and we invest extensive resources in ensuring the supply of safe and secure communication services.

Bezeq's wide-ranging actions to prevent information security incidents

Among other things, we develop methodologies, implement risk management processes, abide by stringent procedures and invest in the human and technological spheres. We strive for innovation and work constantly to introduce the latest advanced technologies.

Our customers rightly rely on us to provide the best, safest and most secure telecommunications experience.

Company policy on information security

In 2011, Bezeq adopted a stringent information security methodology predicated on a protection-oriented outlook that perceives total product and service security as vital for the entire spectrum of the Company's business. Bezeq has a variety of multilevel security solutions specifically designed to limit access to information and monitor its removal.

The Company is overseen by the State Authority for Information Security (SAIS) and is obligated to comply with stringent information security standards based on leading standards in the global telecommunications industry, such as the PCI security standard and ISO 27001 (in 2019 the Company began a process of certification for the standard, which was completed in 2020; until then the Company operated in accordance with the European ISO 270032 standard).

Bezeq appointed a vice president in charge of implementation and compliance with the provisions of the Privacy Protection Law, and it operates in accordance with the directives of the state security bodies. Bezeq has also put in place its own internal procedures (beyond the requirements of the law) and it complies with all the regulatory requirements in the field.

> **Haim Miller, Vice President of Information Security:**
> "The Company applies a protection policy that includes some of the world's most advanced security systems that combine effective security with the Company's operating needs, including multilevel security mechanisms that protect its infrastructure and systems and our customers' information."

Board of directors' involvement in ensuring information security

Once a year the board of directors holds a meeting for the presentation of information security updates. Additionally, a steering committee headed by the CEO convenes annually.

Actions Taken in 2019

1. Preparations to deal with external cyber threats.
2. Preparations to deal with internal cyber attacks.
3. Remote access to the organization.
4. Information security education and awareness within the organization.
5. Bezeq certification for the "Rimon 4" information security level (mandated by the SAIS regulator).

Security Issues

The Company is exposed to "cyber risk," that is, the risk of activity intended to adversely affect computer use or the use of material stored on computers ("cyber attack").

Information and Cyber Security Department

Department's areas of responsibility: information security engineering, assimilation of new technologies, security threat assessments and risk surveys, work plan development, interaction with regulatory authorities, cooperation with the Israel National Cyber Directorate, performance of penetration tests, as well as other activities. Information security activities also are carried out in the Company's different divisions.

The Company monitors the implementation of its information security policy, including examining the level of cyber security effectiveness and the Company's preparedness for cyber security incidents and conducting tests, inspections and exercises.

Employee Training and Involvement

Instruction/Training Programs for Employees

- The Company conducts seven courses that are classified according to jobs (e.g. professional training in different technological areas, secure code development training, a three-day advanced cyber course, etc.). In addition, all employees are required to undergo a tutorial on the subject of information security, with a stress on the protection of privacy and sensitive information, in addition to an information security tutorial that is provided to all newly hired employees of the Company.

- Every year, all the Company's employees are required to participate in ten internal exercises in preparation for various scenarios involving information and cyber security issues such as phishing, introduction of threats to the network through external computers, malware dissemination, and so forth (including through outside companies that specialize in this field).

- In the course of 2019, some 20 emails on information and cyber security were sent to all the Company's employees, dealing with such subjects as secure browsing, increased awareness ahead of cyber attacks, guidelines, policies, etc.

Collaborations

External research organizations- Bezeq collaborates with research companies worldwide on the subject of endpoint security. Senior officers of the Company also attend conferences, in Israel and around the world, to learn about new areas of research and the latest global trends.

Bezeq is collaborating with several Israel startups, among them: SAM - developer of a home network protection system with an emphasis on Internet and IoT products, that is able to secure any device taking its operating system and weaknesses into account.

Customer Privacy

The Company uses data whitening solutions against malicious software through its Security Operations Center (SOC). Its "Bring Your Own Device" (BYOD) technology provides a secure computer environment for people operating in the field. In addition, the Company creates smart IoT-integrated solutions for the performance of monitoring tests.

Cloud Services

Bezeq provides a highly secure cloud platform that complies with the most stringent information security standards, investing substantial resources in the continual upgrading of its information security capabilities and incorporation of new security features.

The Company makes every effort to identify and eliminate in advance privacy breach risks, to strengthen its data protection systems and to improve the control over its distributors, sub-suppliers and subsidiaries, including the provision of instruction.

In 2019, Bezeq revised and upgraded its privacy protection policy and guidelines, to provide better data privacy protection for its customers and employees and all owners of data in general.

The Bezeq website provides customers with updates on information security and privacy protection measures, as required by the Protection of Privacy Law and its regulations.

Below is a description of the array of information and cyber security services provided by Bezeq to Internet users:

Bcyber – real-time reporting of cyber attacks

Bezeq's Bcyber application alerts users directly and in real time to hacking attempts and attacks on the home network or connected devices. Another feature is the "cyber global dashboard" that shows in real time the data on attacks from around the world directed against Israel.

Bezeq estimates that **some 250,000 cyber attacks** against private customers occur daily in Israel, with the number of attacks trending upward.

More than 30,000 cyber attacks against Bezeq customers are **blocked every day.**

Real-time data from Bezeq's Bcyber system show that TV adapters and Android devices are among the most targeted devices.

Service features and capabilities:

- Block access to applications
- Filter and block sites according to child age
- Display current location and arrival and departure alerts
- Receive alerts on the use of offensive language
- Analyze browsing duration and characteristics
- Define Internet and app browsing schedules

Keren Leizerovitch, Vice President of Marketing and Innovation:

"We decided this year to incorporate for the first time younger users because of their dominance on the Web. It appears that these digital native users relate to the virtual space as part of the physical space in which we all live. The data of the report support this and show that the young generation has a stronger presence on the networks, demonstrates responsibility in dealing with network dangers, and treats the content to which it is exposed on the Web with a degree of skepticism."

Safety training and certification at Bezeq includes:

Certification for ladders and flat roofs; certification for work at heights and in confined spaces; certification for work at heights with climbing equipment; certification for restricted electrician's license; first-aid training; certification for operating traffic safety arrangements; certification as safety custodians; general safety training for technicians, etc.

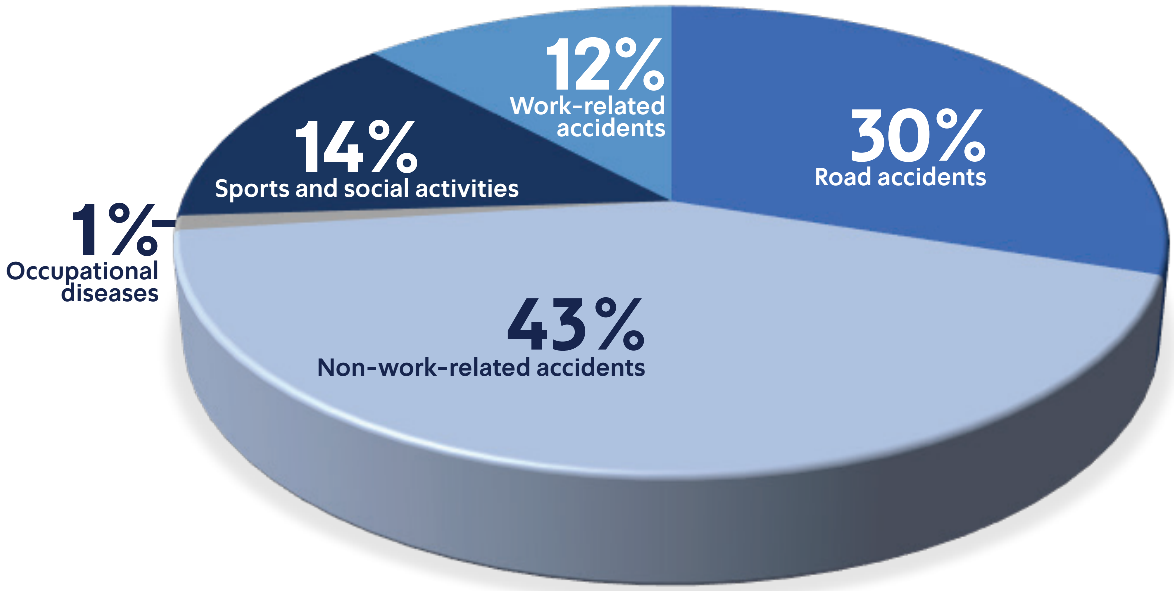
Safety Incidents

Zero disaster incidents in the years 2018-2019

In 2019, 172 accidents of various types (e.g. road accidents, occupational diseases, work-related accidents) were reported by the different divisions. In that year, the number of absence days stood at 5,185 days, and the average number of absence days per accident was 30.1.

In 2018, 180 accidents were reported, the number of absence days stood at 1,705 days, and the average number of absence days per accident was 9.

Types of safety incidents at Bezeq in 2019



Supply Chain

Suppliers

Bezeq worked with approximately 2,700 suppliers in 2019, of which the preponderant majority are local suppliers although a significant proportion of them represent or import from overseas manufacturers. A few tens of the suppliers are key suppliers.

The main fields of business of the suppliers with which Bezeq works include: vehicle leasing, fuel, cables and accessories, telecommunications cabinets, call centers, services, advertising, productions and events, smart business, printing and distribution, surveys and studies, transport services, computer equipment, IT software, storage and servers, information security, building maintenance, energy equipment, security, utilities (Israel Electric Corporation, Paz Oil Refinery Ashdod), catering, etc.

Supplier Preference

Bezeq prefers, whenever possible, to collaborate with socially responsible partners in all fields, be it office equipment, cleaning services, gifts for employees or any other field.

Bezeq often chooses to work with local suppliers. Thus, for example, one of its cable suppliers is a local firm with which Bezeq continues to work in spite of the availability of cheaper alternatives abroad. Additionally, for many years Bezeq has been employing rehabilitation organizations, contributing in this way to the community. Bezeq also regularly purchases holiday gifts for customers from small socially oriented enterprises, such as the Kishor and Tulip wineries in the north of Israel and the Midbar winery in the south.

In 2019 Bezeq collaborated with the Shavim, Northern Goals, Hameshakem and Israeli Public Health non-profit organizations, for a total of NIS 450,000. These organizations carry out works of rendering end equipment and various accessories usable (such as the cleaning of end equipment and sorting of screws, with appropriate packaging).

Our Suppliers' Commitment to the Code of Ethics

Suppliers who contract with Bezeq are required to sign a commitment to comply with its Code of Ethics, including the rules restricting conflicts of interest and prohibiting bribery, In the case of suppliers with a contract value of more than NIS 500,000, the Company also requires them to sign a declaration of no conflict of interest and verifies their compliance with the requirements of the Code of Ethics.

Regarding cleaning, catering and guarding personnel, the Company regularly follows up their terms of employment and checks their wages through external accountants. More information on this subject can be found in the chapter "Employees and Work Environment."

Supplier Engagement

Although Bezeq is not subject to the Mandatory Tenders Law, it nevertheless solicits offers for goods or services from several companies, after conducting a market survey. The Company examines the potential supplier's commercial, technological, business and financial ability to comply with Bezeq's requirements. Companies in the market are invited to approach Bezeq and offer it their products or services on the Procurement Department's website.

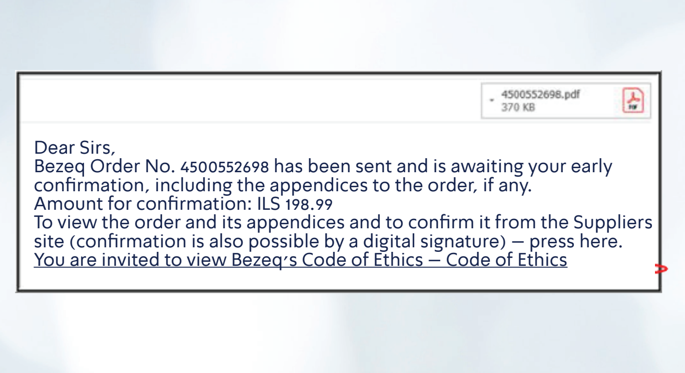
Bezeq conducts meetings with its suppliers and orders reports from various rating agencies. Some 80% of purchases are made by the Procurement Department, and the rest by the Company's other units. Each supplier has a contact person at the Company to whom it can turn on any matter.

Responsible and Green Procurement

In recent years, employment, safety, environmental and human rights considerations have become integral to the procurement process, presenting risks that cannot be ignored. Companies with a complex supply chain and significant procurement processes must maintain a comprehensive policy, dialogue and controls in relation to suppliers, and policy compliance reports must be made to the relevant entities.

Procurement in 2019 amounted to NIS 0.9 billion.

Additionally, in 2019 a significant project of automation of the procurement process was carried out (see details in the chapter "Environmental Responsibility").



Dear Sirs,
Bezeq Order No. 4500552698 has been sent and is awaiting your early confirmation, including the appendices to the order, if any.
Amount for confirmation: ILS 198.99
To view the order and its appendices and to confirm it from the Suppliers site (confirmation is also possible by a digital signature) – press here.
You are invited to view Bezeq's Code of Ethics – Code of Ethics

Challenges for 2020-2021

In the field of information security

We foresee an increase in attacks over the Internet, the leveraging of advanced technology for phishing attacks, the expansion of regulation and enforcement in Israel and around the world on the subjects of privacy and cyber security, cyber-attacks using machine learning and developing artificial intelligence, attacks on and accessing of the organization's resources through the supply chain, etc.

The work plan approved for 2020 was developed taking these challenges into account.

We are continuing to act on all fronts to protect our customers' information and privacy at all times. Among the steps we have taken:

- Completion of Bezeq's certification for ISO 27001
- Management of cyber risks in the IT and engineering systems
- Setup and training of incident response (IR) team
- Consolidation of solutions for the protection of end components
- Secure internal and external browsing for the organization's employees
- Alert in databases regarding leaked identification

In the field of supply chain and suppliers

Increase in and formal prioritization of green and responsible procurement by the Company, with an emphasis on reducing negative impacts on the environment and giving preference to local suppliers.

Formulation of processes and methodologies for measuring the Company's direct negative environmental footprint or the potential footprint through the supply chain.