UZTELECOM

Ensuring the security of personal data and information is our top priority.

The Information Security Policy implemented by the Company is based on international standards and best practices in the industry. We implement modern security technologies in our networks and regularly improve them. Ensuring the security, confidentiality, and integrity of our subscribers' and partners' data is one of our primary goals.

In order to ensure the security of subscribers' data, the Company has developed an Information Security Policy, which outlines the principles, approaches and measures by which data will be reliably protected and the standards established in the field of security will be observed.

Information safety policy of "Uzbektelecom" JSC

"Uzbektelecom" Joint Stock Company (hereinafter referred to as the Company) is the largest telecommunications operator with its network covering all regions of the Republic of Uzbekistan. Using a telecommunications network built on the basis of modern technologies, the Company provides all types of telecommunications services.
The company effectively implements and uses high-tech information and communications in its activities. In such conditions, ensuring information security and cybersecurity is a necessary task. Given the importance of information security, this area has been designated as one of the main functions of the Deputy Chairman of the Board of "Uzbektelecom" JSC for Information Security and Regime. Information security is achieved through the implementation and implementation of a number of measures, such as installing appropriate hardware and software, conducting tests to identify vulnerabilities in networks, organizing training for employees, and regularly monitoring systems. Comprehensive measures to ensure information security ensure the uninterrupted operation of the Company's networks, minimize damage caused by threats, ensure the confidentiality and protection of subscribers' personal data, protect the information and communication infrastructure from various threats, predict and prevent the impact of threats, maintain business reputation and comply with the requirements established by legislative documents.

The Company's Information Security Policy is developed based on the following documents:

The law No 547 "about personal data" dated July 2, 2019 of the Republic of Uzbekistan;
The law No 764 "About cybersecurity" dated April 15, 2022 of the Republic of Uzbekistan;
The decree No PF-6079 "On approval of the "Digital Uzbekistan - 2030" strategy and measures for its effective implementation" dated October 5, 2020 of the President of the Republic of Uzbekistan;

The resolution No PQ-167 “On additional measures to improve the system for ensuring cybersecurity of critical information infrastructure facilities of the Republic of Uzbekistan” dated May 31, 2023 of the President of the Republic of Uzbekistan;
The resolution No 570 “On approval of certain regulatory legal acts in the field of personal data processing” dated October 5, 2022 of the Cabinet of Ministers of the Republic of Uzbekistan;
Uz DSt ISO/IEC 27000:2022 “Information technology. Methods of ensuring security. Information Security Management Systems. Commentary and glossary”;
O‘z DSt ISO/IEC 27001:2020 “Information technology. Methods of ensuring security. Information Security Management Systems. Requirements”;
O‘z DSt ISO/IEC 27002:2016 “Information technology. Methods of ensuring security. Practical rules for information security management”;
Internal regulatory documents developed by the company, relevant action plans.

Goals and tasks

The main objectives of the company's Information Security Policy are to protect the subjects of information relations from material, physical, moral or other harm, accidental or intentional unauthorized interference in the activities of informatization objects or unauthorized access to and illegal use of information contained therein, eliminate and minimize the possible consequences of information security incidents, predict and prevent threats, identify and eliminate vulnerabilities in information systems, ensure the compliance with the requirements set forth in legislative documents, instructions, and regulations in the field of information security, ensure that the company's information resources are backed up and restored.

The most important task is to prevent and detect unauthorized access to the Company's information facilities, identify and eliminate vulnerabilities in the Company's information resources and information security management systems, ensure that all Company employees are attentive to information security, provide information about any potential threats, and keep confidential information and trade secrets, as well as personal data of customers, confidential.

Today, the Company is working not only in the field of information security and cybersecurity, but also to ensure the safety of you and your loved ones. An example of this is the Company's services "Kid security", "Dr.Web - anti-virus solution".

Information security measures

The Company's internal regulatory documents in the field of information security are developed and maintained by the Company's Security Department. Internal regulatory documents on information security and the requirements set forth therein are communicated to all employees of the Company by the Security Department, and employees work in strict compliance with the established requirements.

The company regularly carries out relevant work to protect and not disclose confidential information, create and develop information protection systems and tools, and improve the skills and awareness of employees in the field of information security.

The company's Security Department oversees the performance of tasks assigned to corporate network, system, and information security administrators.

The company's security service organizes quarterly inventory work on information security in local networks and on computers at employees' workplaces and is carried out as part of internal audits. If appropriate measures need to be taken based on the results of the inventory, the necessary work is carried out.

Corporate email data, official website data, file server, main server domain controller settings and data, information security tools settings and databases in the company's information systems and resources are regularly monitored.

To ensure the reliability (security) of information system data, RAID data storage systems of primary and backup data centers are used.

To ensure physical protection of data, database servers and data storage systems are located in a secure server room in the Company's Data Center (DataCentre).

Non-disclosure agreements are signed with employees with employment contracts, as well as with partners with whom contracts for the provision of services and relevant purchases have been concluded.

Employees responsible for ensuring information security in the Company regularly participate in various seminars and conferences to improve their skills in this area, and training is provided to all employees of the Company to comply with the requirements of the Information Security Policy.

Response to information security incidents

Key tasks of the information security incident management process:

Minimize losses, including rapid incident detection and reduce the risk of recurring incidents;

Rapid identification, analysis, and registration of information security incidents, notification of authorized bodies regarding information security incidents, identification of sources and causes of incidents, and consideration of their consequences;

Minimize damage to the company's information resources, prevent the disclosure of subscriber data, restore information resources, the corporate network and information resources in the event of their failure as a result of an information security incident in a short time, and analyze the results of eliminating the consequences of an information security incident and take appropriate measures;

The company must take appropriate measures to prevent the recurrence of incidents related to the information security of information resources and carry out the necessary work in cooperation with the State Enterprise "Cybersecurity Center" on information security incidents.

“Uzbektelecom JSC” constantly carries out and improves extensive work to ensure information security.

UZTELECOM -
your data is under reliable protection..