Development of Fixed Wireless Access (FWA) in Rural Areas

The subsidiary Auyl Telecom LLP is implementing pilot projects to develop fixed wireless access (FWA) in rural areas, providing high-speed internet in locations where the construction of fibre-optic communication lines (FOCL) or GPON networks is economically unfeasible. This initiative helps reduce the digital divide and deliver modern connectivity to residents of remote regions.

As part of the pilot projects, solutions based on Open RAN and 5G FWA have already been tested. In the village of Sarybay, the average connection speed increased 85-fold – from 5 Mbps to 427 Mbps – significantly improving the quality of online education, telemedicine, and remote work. Thus, FWA not only modernises outdated technologies (WiFi, ADSL, CDMA EVDO) but also becomes a key tool in bridging the digital gap between urban and rural areas.

Auyl Telecom continues to actively expand its FWA network, with 5G being a strategic focus for the company. However, a 4G network is also being developed in parallel. A successful example of implementation is the village of Karatala in the Aktobe region, where 79 out of 120 households have been connected. The average connection speed is 46 Mbps, and the average internet traffic consumption per household over a three-week period reached 191 GB. For 10 subscribers, the data usage exceeded 450 GB during the same period.

Testing of various network functions and technical solutions

- The technical feasibility and readiness of the hardware and software complex based on Open RAN 5G Fronthaul for providing Internet access via fixed wireless access were tested. The operability of the Open RAN 5G Fronthaul solution was confirmed with some limitations.
- The invGUARD AS-SW software suite was tested to evaluate its capabilities in monitoring and analyzing network traffic statistics on the Kazakhtelecom JSC network within the TelcoCloud environment.
- The VOLTHA GPON technology was tested in the TelcoCloud environment in the city of Konaev. The main idea of this solution is disaggregation and avoidance of vendor lock-in. In traditional GPON, OLT (stationary equipment), software, licenses, and ONT (customer premises equipment) are supplied by a single vendor and are “locked,” which prevents connecting ONTs from other manufacturers to an OLT of a different vendor or using software from other providers. The VOLTHA solution overcomes these restrictions by allowing the selection of white-box OLT hardware from one manufacturer, software and licenses from another, and using the openOMCI standard to connect ONTs from different vendors.
- The product is not yet fully ready, but the concept and implementation activity are already delivering results. The pilot broadband project based on VOLTHA is currently being implemented in Konaev.
- The service of providing access to cache servers for telecom operators in Kazakhstan and Central Asia was tested.
- Testing has begun on an indoor solution to provide mobile Internet access using PicoCell in locations with poor mobile/broadband signal quality (e.g., shops, cafes located in basements).

INFORMATION SECURITY AND DATA PROTECTION

The Company recognises the importance of ensuring information security and protecting its clients’ data. Kazakhtelecom JSC continues to develop a robust information security and data protection management system.

MANAGEMENT APPROACH

GRI 3-3, 418-1

The Information Security Service reports directly to the Managing Director for Information Security, who oversees information security issues at the highest level within the Company.

The key internal documents regulating information security include:

- Information Security Policy;
- Personal Data Protection Policy of Kazakhtelecom JSC;
- Information Security Concept.

These documents are available on the Company’s website in the “Sustainable Development” section, under the “Information Security and Data Protection” subsection.

Key principles of information security management:

- compliance with legal requirements;
- involvement of top management in the information security process;
- business orientation;
- process-based approach;
- comprehensive use of methods, tools, and means of protection;
- adherence to best practices;
- reasonable sufficiency;
- awareness and personal accountability.

To ensure information security, Kazakhtelecom JSC applies a systematic approach. One of the key aspects is round-the-clock monitoring of data throughout their entire lifecycle – from the moment they enter the Company’s infrastructure to their archiving or permanent deletion.

Currently, the Company applies globally recognized best practices in information security. Internal systems are protected using solutions such as secure remote access to information resources, safe internet usage, privileged access management (PAM), vulnerability scanners, and more. The Company strives to counter external threats and implements new solutions and methods for handling resources, including the development of internal infrastructure, training of qualified specialists, the establishment of a Security Operations Center (SOC), and the adoption of the Zero Trust concept.

Other important security components used by the Company include integration into the national cybersecurity system (YShDI), Internet of Things (IoT) security, deployment of honeypots, the use of machine learning, and other advanced technologies. In addition, regular training and awareness-raising activities are conducted to enhance employees’ knowledge of information security.

Personal Data Protection

GRI 418-1

The Company has developed and implemented the Personal Data Protection Policy, which sets out the core principles for processing the personal data of clients, suppliers, business partners, employees, and other individuals. It defines the key actions related to the collection, storage, and processing of personal data, as well as the measures taken to protect such data.

This Policy serves as the fundamental document in the field of personal data protection, establishing the objectives, tasks, and principles the Company adheres to in its operations. It also provides a framework for the development of other related internal documents.

Key principles of personal data protection:

- respect for constitutional rights and freedoms of individuals and citizens;
- legality of personal data protection processes;
- confidentiality of restricted-access personal data;
- engagement of the Company's management in ensuring personal data protection;
- business orientation;
- process-based approach;
- comprehensive application of tools, methods, and means of protection;
- alignment with best practices;
- reasonable sufficiency;
- awareness and personal responsibility.

Key Results for the Reporting Period

In 2024, the Company implemented a comprehensive set of measures in the area of information security to protect corporate information systems, personal data, confidential information, and data transmission networks.

As part of maintaining an up-to-date information security management system, the Company approved 16 regulatory and procedural documents.

To raise awareness among Kazakhtelecom employees regarding information security, the Company issued 7 informational newsletters, launched 2 digital marathons on the Corporate University training portal covering rules and requirements in the area of information security, and conducted 4 cybersecurity drills in the form of phishing simulations to assess employees' cyber hygiene and response actions to suspicious emails.

A comprehensive inspection was carried out across facilities and server rooms housing equipment classified as critical information communication infrastructure (CICI), along with the structural units responsible for their administration. Based on identified non-conformities, recommendations were issued to heads of relevant departments.

As part of operational improvements, the Company's IT Division reorganized internal departments in 2024 to launch a corporate Security Operations Center (SOC) and switch to 24/7 operations. The SOC is responsible for:

- Protecting the Company's corporate perimeter;
- Monitoring information security (IS) events;
- Responding to IS incidents;
- Investigating IS incidents;
- Identifying vulnerabilities in the Company's information systems;
- Issuing recommendations for resolving IS incidents;
- Monitoring the effectiveness of information protection tools.

In 2024, the second phase of the Company's transition to the ZeroTrust model was completed. A range of hardware and software security tools were deployed, significantly strengthening the Company's corporate infrastructure protection. Key results of the corporate SOC in 2024:

- Approximately 3,300 DDoS attacks on customer resources were repelled (peak intensity exceeding 74 Gbps), with total malicious traffic over 1,100 Tb;
- Over 710 million malicious traffic packets were blocked;
- Software vulnerability scanners detected around 118,000 vulnerabilities in company systems, over 64% of which were remediated by responsible administrators;
- More than 40,000 network attacks were neutralized via protection tools, along with detection of 45,000 viruses and blocking of over 20,000 password brute-force attempts;
- The Privileged Access Management (PAM) system monitored more than 270 privileged users (system administrators, external users, and contractors) across over 120 terminal server IP addresses used for accessing corporate information systems;
- Data Leak Prevention (DLP) systems detected over 800 files containing confidential information stored in violation of internal security requirements;
- Around 60 honeypots (decoy systems simulating real company assets) were deployed, which helped detect more than 2,000 malicious requests within the corporate network.

During the reporting period, one hotline report was received concerning a potential personal data processing violation. The investigation did not confirm any client data breach. No confirmed incidents of customer data leaks were recorded during the period.

Employee Awareness and Training on Information Security

GRI 418-1

The Company conducts regular training activities for its employees to uphold the core principles of information security – confidentiality, integrity, and data availability.

Information security is ensured at multiple levels. Administratively, every employee is required to review and comply with the Company's internal regulations, rules, and policies in the field of information security. Technically and physically, the Company applies a range of hardware and software systems, including cryptographic protection tools and other security measures.

In addition, specialists from the Information Security Division regularly undergo various advanced training courses on information security, cybersecurity, and information security risks and threats. General training and testing on digital hygiene are conducted for employees in customer service and HR departments, where the risk of unauthorized data use is relatively high.