Technical Security

1. General Provisions

1.1. This Technical Security Policy of InfraTech (hereinafter referred to as the "Policy") outlines the main measures for protecting data and ensuring the secure operation of the website “infratech.kz” (hereinafter referred to as the "Website").

1.2. The Policy aims to prevent unauthorized access, data breaches, and other threats that could impact the functionality of the Website and the protection of user information.

1.3. The company reserves the right to update this Policy by publishing the revised version on the Website.

1.4. Users are responsible for monitoring updates to the Policy.

1.5. By using the Website, the User acknowledges and agrees to the terms of this Policy in full. If the User disagrees with any provisions, they must cease using the Website.

2. Data and Technology Protection

2.1. The company implements modern data protection measures, including:

Encryption of data during transmission and storage using SSL/TLS protocols.

Encryption of data during transmission and storage using SSL/TLS protocols.

Regular updates of software and security systems.

Regular updates of software and security systems.

Monitoring and analyzing suspicious activity to prevent threats.

Monitoring and analyzing suspicious activity to prevent threats.

2.2. Access to data is strictly limited to authorized company personnel.

2.3. Multi-layered security systems, such as firewalls, antivirus software, and intrusion detection/prevention systems (IDS/IPS), are in place.

3. Access Management

3.1. The company enforces multi-factor authentication (MFA) to protect user accounts.

3.2. Each user is provided with unique credentials that are encrypted for additional security.

3.3. Unauthorized access to data or systems is automatically blocked.

4. Backup and Recovery

4.1. Regular backups of data are performed to prevent its loss.

4.2. Backups are stored in secure locations inaccessible to unauthorized access.

4.3. Recovery mechanisms ensure minimal system downtime in the event of unforeseen circumstances.

5. Vulnerability Detection and Mitigation

5.1. The company conducts regular security audits to identify potential vulnerabilities.

5.2. We collaborate with professional organizations to perform penetration testing and assess our security measures.

5.3. If a threat is detected, the company takes immediate action to address it.

6. Responsibility for Security

6.1. We adhere to international security standards, including ISO/IEC 27001, PCI DSS, and others.

6.2. The company provides ongoing training for its employees on information security best practices.

7. Reporting Security Issues

7.1. If you discover a vulnerability on our Website or suspect a security threat, please contact us at info@infratech.kz.

7.2. All security-related reports are reviewed promptly, and appropriate actions are taken as quickly as possible.

8. Policy Updates

8.1. The Technical Security Policy may be updated to meet new standards and requirements.

8.2. The updated version of the Policy will be published on the Website and will take effect upon publication.

9. Contact Information

9.1. For questions related to technical security, please contact us at: info@infratech.kz.

Our primary goal is to ensure a safe and reliable experience for all Website users.