

INFORMATION SECURITY POLICY

Dehqonobod Kaliy Zavodi JSC

1. PURPOSE

The purpose of this Information Security Policy is to protect the confidentiality, integrity, and availability of Dehqonobod Kaliy Zavodi JSC's information assets against unauthorized access, misuse, loss, or damage. The Policy defines the framework and responsibilities for ensuring the secure management of all information and IT systems within the company.

2. SCOPE

This Policy applies to all employees, contractors, consultants, and third parties who access, process, or store information owned or managed by Dehqonobod Kaliy Zavodi JSC, regardless of location or medium (digital or physical).

3. OBJECTIVES

- To ensure that information is protected from unauthorized access or disclosure;
- To maintain the accuracy and completeness of data;
- To ensure that information and systems are available to authorized users when required;
- To comply with applicable national regulations, company procedures, and international standards;
- To promote awareness and accountability among employees for information security.

4. GOVERNANCE AND RESPONSIBILITIES

- The IT Department is responsible for implementing and maintaining the company's information security controls and procedures.
- The Information Security Officer (ISO) oversees compliance with this Policy and reports to the Deputy Chairman for Technical Affairs.
- The Management Board provides oversight and ensures that adequate resources are allocated for information security.
- All employees and contractors must comply with this Policy and report any suspected breaches or incidents.

5. INFORMATION SECURITY CONTROLS

The company maintains the following key control measures:

1. Access Control: Access to systems and data is granted on a need-to-know basis and protected by user authentication.
2. Data Protection: Sensitive information is stored securely, encrypted where appropriate, and regularly backed up.
3. Network Security: Firewalls, antivirus, and intrusion detection systems are implemented to protect the IT infrastructure.
4. Incident Response: A defined process exists to detect, report, and respond to security incidents.
5. Physical Security: Access to server rooms and critical infrastructure is controlled and monitored.
6. Awareness Training: Regular training sessions are provided to employees on cybersecurity and safe data handling.

6. COMPLIANCE

All information security practices must comply with:

- National data protection and cybersecurity regulations of the Republic of Uzbekistan;
- ISO/IEC 27001 Information Security Management System standards;
- Internal company procedures and ethical standards.

7. REVIEW AND UPDATE

This Policy shall be reviewed annually or whenever significant changes occur in the company's IT infrastructure or regulatory requirements.

8. APPROVAL

This Information Security Policy has been approved by the Management Board of Dehqonobod Kaliy Zavodi JSC and is effective as of the date of approval.

Approved by:

Chairman of the Management Board

Dehqonobod Kaliy Zavodi JSC