INFORMATION SECURITY POLICY

THE POLICY HAS BEEN APPROVED BY THE DECISION OF THE SCIENTIFIC COUNCIL OF NAKHCHIVAN STATE UNIVERSITY AT THE MEETING HELD ON JULY 1, 2023 (PROTOCOL NO: 01), AND REVIEWED ON JANUARY 6, 2025.

CONTACT US

strategy@ndu.edu.az
www.ndu.edu.az

NAXÇIVAN DÖVLƏT UNİVERSİTETİ

1. Purpose

This Information Security Policy defines the general principles for protecting information assets at Nakhchivan State University (NSU).

The objective of this policy is to support the confidentiality, integrity, and availability of institutional information used in academic, administrative, and digital services.

This policy provides a framework for managing information security risks and promoting secure and responsible use of information systems.

2. Scope

This policy applies to:

- All students, academic staff, administrative personnel, and authorised third parties
- University-managed information systems and digital platforms
- Academic, administrative, and research data
- IT infrastructure, networks, and related services
- Any systems or services operated on behalf of the university

3. Information Security Objectives

NSU aims to:

- Protect information assets against unauthorised access, alteration, or disclosure
- Ensure the reliability and accuracy of institutional information
- Maintain the availability of critical systems and services
- Support secure and responsible use of digital resources
- Reduce information security risks to an acceptable level

4. Reference Frameworks

This policy is developed with reference to widely recognised international standards and best practices, including:

- ISO/IEC 27001 (Information Security Management Systems – Requirements)
- ISO/IEC 27002 (Information Security Controls – Code of Practice)
- ISO/IEC 27701 (Privacy Information Management – where applicable)

The policy also considers relevant national legislation and internal university regulations.

5. Information Security Principles

5.1 Confidentiality

Information shall be accessible only to authorised individuals. unauthorised disclosure or access is not permitted.

5.2 Integrity

Information shall be protected against unauthorised modification or destruction. Accuracy and completeness of data shall be maintained.

5.3 Availability

Information and systems shall be available to authorised users when required, subject to operational and technical constraints.

6. Access Control

Access to information systems shall be managed based on:

- Identification and authentication mechanisms
- Role-based access control principles
- The principle of least privilege
- Regular review and adjustment of access rights

Users are responsible for safeguarding their authentication credentials.

7. Information Asset Management

Information assets shall be:

- Identified and documented
- Classified according to sensitivity and importance
- Protected according to their classification level
- Managed throughout their lifecycle (creation, use, storage, archival, disposal)

8. Data Protection

The university applies appropriate measures to protect personal and institutional data, including:

- Limiting data collection to legitimate purposes
- Ensuring access is restricted to authorised personnel
- Preventing unauthorised disclosure or misuse
- Applying appropriate backup and recovery practices where necessary

9. User Responsibilities

All users of university information systems shall:

- Use systems in a lawful, ethical, and responsible manner
- Protect personal login credentials and access information
- Avoid unauthorised access attempts or misuse of systems
- Report suspected security incidents promptly
- Comply with applicable policies and procedures

10. IT Governance and Responsibilities

The university is responsible for the following:

- Defining and maintaining information security policies
- Implementing appropriate security controls
- Managing information security risks
- Monitoring compliance with security requirements
- Coordinating incident response activities
- Supporting continuous improvement of security practices

11. Information Security Incident Management

Information security incidents may include, but are not limited to:

- unauthorised access attempts
- Data breaches or suspected data leakage
- System disruption or service unavailability
- Malicious software or cyberattacks

All incidents shall be:

- Reported through designated channels
- Assessed for impact and severity
- Managed through appropriate containment and mitigation actions
- Documented for review and improvement purposes

12. Business Continuity

The university shall take reasonable measures to support the continuity of critical services, including:

- Identification of essential systems and services
- Implementation of recovery and continuity planning approaches
- Periodic review of continuity arrangements
- Minimisation of disruption to academic and administrative operations

13. Compliance

This policy is developed with reference to internationally recognised standards, including ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701 (where applicable).

It also takes into account relevant national legislation and internal institutional regulations.

14. Continuous Improvement

NSU is committed to maintaining and improving its information security practices through:

- Periodic policy reviews
- Risk assessments and evaluations
- Adaptation to emerging security threats
- Awareness and training activities

15. Final Statement

This policy establishes the general framework for information security at Nakhchivan State University and supports the secure, reliable, and responsible use of information systems across the institution.