ISSN 2181-

KOMPANIYALARDA AXBOROT XAVFSIZLIGI SIYOSATINI ISHLAB CHIQISH VA JORIY ETISH

DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY POLICY IN COMPANIES

O'zbekiston Respublikasi IIV Akademiyasi kunduzgi ta'lim
3-o'quv kursi 333-guruh kursanti
Rahmatullayeva Ruhshona Oybek qizi

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
cadet of group 333 of the 3rd year of study
Rahmatullayeva Ruhshona Oybek qizi

A N N O T A T S I Y A

Maqolada O'zbekiston Respublikasining amaldagi qonunchilik hujjatlari talablariga to'liq mos keladigan axborot xavfsizligi siyosatini (AXS) ishlab chiqish va joriy etishning huquqiy, tashkiliy va amaliy jihatlari atroflicha yoritilgan. "Axborotlashtirish to'g'risida"gi, "Shaxsiy ma'lumotlar to'g'risida"gi qonunlar, Prezidentning 15.04.2021 yildagi PQ-5082-son qarori hamda boshqa normativ-huquqiy hujjatlar talablari tahlil qilinib, majburiy hujjatlar ro'yxati, mas'uliyatlar taqsimoti va nazorat mexanizmlari keltirilgan.

A B S T R A C T

The article thoroughly examines the legal, organizational and practical aspects of developing and implementing an Information Security Policy (ISP) that fully complies with the current legislation of the Republic of Uzbekistan. The requirements of the Law "On Informatization", the Law "On Personal Data", Presidential Decree

No. PQ-5082 dated 15 April 2021 and other normative-legal acts are analyzed; the list of mandatory documents, distribution of responsibilities and control mechanisms are presented.

Kalit so‘zlar: axborot xavfsizligi siyosati, shaxsiy ma’lumotlar, kritik axborot infratuzilmasi, PQ-5082, O‘zbekiston qonunchiligi, axborot xavfsizligi boshqaruv tizimi.

Keywords: information security policy, personal data, critical information infrastructure, PQ-5082, legislation of Uzbekistan, information security management system.

1. Kirish

O‘zbekiston Respublikasida raqamlashtirish jarayoni tezlashmoqda. 2020–2030 yillarga mo‘ljallangan “Raqamli O‘zbekiston-2030” strategiyasi doirasida davlat organlari, banklar, korxonalar va fuqarolar o‘rtasida elektron hujjat aylanishi kengaymoqda. Shu bilan birga, axborot xavfsizligi buzilishi holatlari ham ortib bormoqda.

O‘zbekiston Respublikasi qonunchiligiga ko‘ra, ayrim turdagi tashkilotlar uchun axborot xavfsizligi siyosatini ishlab chiqish va doimiy yangilab borish majburiydir. Ushbu maqola aynan O‘zbekiston qonunchiligi talablariga asoslangan holda korxonalar uchun to‘g‘ri va qonuniy AXS yaratish bo‘yicha to‘liq yo‘riqnoma hisoblanadi.

1.Introduction

Digitalization processes are accelerating in the Republic of Uzbekistan. Within the framework of the “Digital Uzbekistan-2030” strategy for 2020–2030, electronic document circulation between state bodies, banks, enterprises and citizens is expanding. At the same time, incidents of information security breaches are increasing.

According to the legislation of the Republic of Uzbekistan, certain types of organizations are obliged to develop an information security policy and keep it up to date. This article serves as a comprehensive guideline for enterprises on creating a correct and lawful ISP based solely on the requirements of national legislation.

2. O‘zbekiston qonunchiligidagi asosiy majburiyatlar

№ Normativ-huquqiy hujjat | Majburiy talablar.

1.“Axborotlashtirish to‘g‘risida”gi Qonun (O‘RQ-639, 17.09.2020) | 17-moddada axborot xavfsizligini ta’minlash choralarini ko‘rish majburiyati belgilangan |

2. “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun (O‘RQ-547, 02.07.2019) | 15–18-moddalar: shaxsiy ma’lumotlarni qayta ishlaydigan har qanday operator ichki siyosat va tartib-qoidalarni ishlab chiqishi shart |

3.PQ-5082-son qaror (15.04.2021) | Axborot xavfsizligi siyosati, hodisalarga javob berish rejasi, xodimlarni o‘qitish dasturi majburiy hujjatlar ro‘yxatiga kiritilgan |

4. Vazirlar Mahkamasining 2023-yil 12-son qarori | Kritik axborot infratuzilmasi ob’ektlari uchun alohida qattiq talablar |

5.Markaziy bankning 32/4-son nizomi (2022) | Barcha bank va moliya tashkilotlari uchun AXS mavjudligi va yillik audit majburiy |

6. “Elektron tijorat to‘g‘risida”gi Qonun | Internet-do‘konlar va to‘lov tizimlari uchun mijozlar ma’lumotlarini himoya qilish siyosati talab etiladi |

Yuqoridagi hujjatlarga ko‘ra, quyidagi tashkilotlar AXS ishlab chiqishga majbur:

- banklar va moliya tashkilotlari
- shaxsiy ma’lumotlarni qayta ishlaydigan barcha operatorlar (HR, buxgalteriya, CRM, onlayn-do‘konlar, mobil ilovalar)
- davlat axborot tizimlari va resurslari operatorlari
- kritik axborot infratuzilmasi ob’ektlari (energetika, transport, aloqa)
- litsenziya yoki ruxsatnoma asosida faoliyat yurituvchi ko‘pgina korxonalar

No.	Normative-legal act	Mandatory requirements (summary)
1	Law “On Informatization” (No. ZRU-639, 17.09.2020)	Article 17 establishes the obligation to take measures to ensure information security
2	Law “On Personal Data” (No. ZRU-547, 02.07.2019)	Articles 15–18: any personal data operator must develop internal policies and procedures
3	Presidential Decree No. PQ-5082 (15.04.2021)	Information security policy, incident response plan and employee training program are included in the list of mandatory documents
4	Resolution of the Cabinet of Ministers No. 12 of 2023	Special strict requirements for objects of critical information infrastructure
5	Regulation of the Central Bank No. 32/4 (2022)	Availability of ISP and annual audit are mandatory for all banks and financial organizations
6	Law “On Electronic Commerce”	Online shops and payment systems are required to have a policy for protecting customer data

According to the above documents, the following organizations are obliged to develop an ISP:

– banks and financial organizations;

– all operators processing personal data (HR, accounting, CRM systems, online shops, mobile applications);

– operators of state information systems and resources;

– objects of critical information infrastructure (energy, transport, communications);

– most enterprises operating on the basis of licenses or permits.

3. O‘zbekiston qonunchiligiga mos Axborot xavfsizligi sohasining majburiy tarkibiy qismlari (PQ-5082 talabi bo‘yicha)

O‘zbekiston qonunchiligida to‘g‘ridan-to‘g‘ri “Axborot xavfsizligi siyosati” hujjatining shakli va mazmuni uchun shablon berilmagan, lekin quyidagi bo‘limlar majburiydir:

1. Kirish qismi va qamrov doirasi

2. Rahbariyatning majburiyati va qo‘llab-quvvatlashi
3. Axborot xavfsizligi maqsadlari
4. Tashkiliy choralar (mas’ul shaxslar, vakolatlar)
5. Texnik va dasturiy choralar (parollar, shifrlash, antivirus)
6. Fizik xavfsizlik choraları
7. Shaxsiy ma’lumotlarni himoyalash bo‘yicha maxsus qoidalar
8. Xodimlarni o‘qitish va xabardor qilish tartibi
9. Axborot xavfsizligi hodisalariga javob berish rejasi
10. Siyosatni buzganlik uchun javobgarlik va sanksiyalar
11. Siyosatni muntazam ko‘rib chiqish va yangilash tartibi

3. Mandatory components of the Information Security Policy in accordance with Uzbekistan legislation (requirements of PQ-5082)

The legislation of Uzbekistan does not provide a direct template for the “Information Security Policy” document, but the following sections are mandatory:

1. Introduction and scope
2. Management commitment and support
3. Information security objectives
4. Organizational measures (responsible persons, authorities)
5. Technical and software measures (passwords, encryption, antivirus)
6. Physical security measures
7. Special rules for personal data protection
8. Procedure for employee training and awareness
9. Incident response plan
10. Liability and sanctions for policy violation
11. Procedure for regular review and updating of the policy

4. O‘zbekiston sharoitida AXS ishlab chiqishning bosqichma-bosqich rejasi

Bosqich 1. Rahbariyatdan rasmiy topshiriq olish (buyruq chiqarish)

Bosqich 2. Axborot xavfsizligi bo‘yicha mas’ul shaxsni tayinlash (buyruq bilan)

Bosqich 3. Ishchi guruh tuzish (IT, yuridik, kadrlar, buxgalteriya vakillari)

Bosqich 4. Axborot aktivlari va shaxsiy ma’lumotlar ro‘yxatini tuzish

Bosqich 5. Xavf-xatarlarni aniqlash va baholash (oddiy jadval shaklida ham bo‘ladi)

Bosqich 6. Majburiy hujjatlar to‘plamini ishlab chiqish:

- Axborot xavfsizligi siyosati
- Shaxsiy ma’lumotlarni himoyalash tartibi
- Hodisalarga javob berish rejasi
- Zaxira nusxalash va qayta tiklash rejasi
- Parollar va huquqlarni boshqarish qoidalari
- Masofaviy ish va BYOD qoidalari

Bosqich 7. Rahbariyat tomonidan tasdiqlash

Bosqich 8. Barcha xodimlarga tanishtirish (imzo qo‘yiladigan jurnal)

Bosqich 9. Yillik ichki tekshiruv va rahbariyat ko‘rib chiqishi

4. Step-by-step plan for developing an ISP under Uzbekistan conditions

Stage 1. Obtaining an official assignment from management (issuing an order)

Stage 2. Appointment of a person responsible for information security (by order)

Stage 3. Formation of a working group (representatives of IT, legal, HR and accounting departments)

Stage 4. Compilation of registers of information assets and personal data

Stage 5. Identification and assessment of risks and threats (can be in simple table form)

Stage 6. Development of the mandatory set of documents:

– Information Security Policy

– Personal Data Protection Procedure

– Incident Response Plan

– Backup and Recovery Plan

– Password and Access Rights Management Rules

– Remote Work and BYOD Rules

Stage 7. Approval by management

Stage 8. Familiarization of all employees (with signature in the register)

Stage 9. Annual internal audit and management review

5. To‘liq namunaviy hujjat (O‘zbekiston qonunchiligiga mos)

[Kompaniya nomi] MChJ

Buyruq № ___ “___” _____ 2025 y.

AXBOROT XAVFSIZLIGI SIYOSATI

1. Umumiy qoidalar

1.1. Ushbu Siyosat O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi, “Shaxsiy ma’lumotlar to‘g‘risida”gi qonunlari hamda PQ-5082-son qaror talablariga asosan ishlab chiqilgan.

1.2. Siyosat kompaniyaning barcha xodimlari, shartnoma asosidagi pudratchilar va uchinchi tomonlar uchun majburiydir.

2. Maqsad va qamrov

2.1. Kompaniya faoliyatida foydalaniladigan barcha axborot aktivlari (shu jumladan shaxsiy ma’lumotlar) maxfiyligi, yaxlitligi va mavjudligini ta’minlash.

2.2. Siyosat kompaniyaning barcha bo‘linmalari, filiallariga va masofaviy xodimlariga tatbiq etiladi.

3. Rahbariyat majburiyati

Rahbariyat axborot xavfsizligini ta’minlash uchun zarur moliyaviy, texnik va kadr resurslarini ajratishga majburdir.

4. Mas’uliyatlar

- Axborot xavfsizligi bo‘yicha mas’ul shaxs: _____ (F.I.O., lavozimi)
- Har bir bo‘lim boshlig‘i o‘z bo‘limidagi axborot aktivlari uchun javobgardir
- Har bir xodim o‘ziga ishonib topshirilgan ma’lumotlar xavfsizligi uchun shaxsiy javobgardir

5. Asosiy qoidalar

5.1. “Toza stol va toza ekran” qoidasi

5.2. Parol siyosati: kamida 10 belgi, katta-kichik harf, raqam va maxsus belgi

5.3. Shaxsiy ma’lumotlar faqat shifrlangan holda saqlanadi va uzatiladi

5.4. Antivirus dasturi majburiy, avtomatik yangilanishi ta’minlanadi

5.5. Masofaviy kirish faqat VPN orqali

5.6. Ma’lumotlarning zaxira nusxasi haftada kamida 1 marta olinadi

5.7. Shaxsiy ma’lumotlarga kirish huquqi “zaruriyat prinsipi” asosida beriladi

6. Xodimlarni o‘qitish

Har yili kamida 1 marta axborot xavfsizligi bo‘yicha o‘quv seminari o‘tkaziladi (bayonnoma bilan).

7. Hodisalarga javob berish

Axborot xavfsizligi hodisasi yuz berganda 24 soat ichida mas’ul shaxsga xabar beriladi va maxsus shaklda qayd etiladi.

8. Javobgarlik

Siyosat talablarini buzganlik uchun O‘zbekiston Respublikasi Mehnat kodeksining 184–187-moddalariga muvofiq intizomiy, moddiy va ma’muriy javobgarlik qo‘llaniladi.

9. Siyosatni ko‘rib chiqish

Siyosat har yili yoki qonunchilikda o‘zgarishlar yuz berganda qayta ko‘rib chiqiladi.

Direktor: _____ /F.I.O./

M.O‘.

5. Full sample document (fully compliant with Uzbekistan legislation)

[Company Name] LLC

Order No. ___ dated “___” _____ 2025

INFORMATION SECURITY POLICY (Developed in accordance with the legislation of the Republic of Uzbekistan)

1. *General Provisions*

1.1. This Policy has been developed in accordance with the Laws of the Republic of Uzbekistan “On Informatization”, “On Personal Data” and Presidential Decree No. PQ-5082.

1.2. The Policy is mandatory for all employees of the company, contractors and third parties.

2. *Purpose and Scope*

2.1. To ensure confidentiality, integrity and availability of all information assets used in the company’s activities (including personal data).

2.2. The Policy applies to all divisions, branches and remote employees of the company.

3. *Management Commitment*

Management is obliged to allocate the necessary financial, technical and human resources to ensure information security.

4. *Responsibilities*

– Person responsible for information security: _____ (full name, position) – Each department head is responsible for information assets in his/her department

– Every employee is personally responsible for the security of information entrusted to him/her

5. *Basic Rules (mandatory)*

5.1. “Clean desk and clean screen” rule

5.2. Password policy: minimum 10 characters, upper and lower case letters, numbers and special characters

5.3. Personal data are stored and transmitted only in encrypted form

5.4. Antivirus software is mandatory with automatic updates

5.5. Remote access only via VPN

5.6. Data backups at least once a week

5.7. Access to personal data is granted on the “need-to-know” principle

6. *Employee Training*

At least once a year, a training seminar on information security is conducted (with minutes).

7. *Incident Response*
8. In case of an information security incident, the responsible person must be notified within 24 hours and the incident recorded in a special form.
9. *Liability*

Violation of the Policy requirements entails disciplinary, material and administrative liability in accordance with Articles 184–187 of the Labor Code of the Republic of Uzbekistan.

10. *Policy Review*

The Policy is reviewed annually or when changes occur in legislation.

Director: _____ /Full name/

Seal

6. Xulosa

O‘zbekiston Respublikasi qonunchiligiga ko‘ra, axborot xavfsizligi siyosati faqat “yozib qo‘yiladigan” hujjat emas, balki rahbariyat tomonidan doimiy qo‘llab-quvvatlanadigan va xodimlar tomonidan bajariladigan majburiy ichki qonun hisoblanadi. Ushbu maqolada keltirilgan talablar va namunaviy hujjat har qanday yuridik shaxs tomonidan bevosita qo‘llanilishi mumkin va davlat organlari, banklar, auditorlar tekshiruvida to‘liq qabul qilinadi.

6. Conclusion.

According to the legislation of the Republic of Uzbekistan, the information security policy is not just a formal document; it is an internal law that must be continuously supported by management and strictly observed by employees. The requirements and sample document provided in this article can be directly applied by any legal entity and will be fully accepted during inspections by state bodies, banks and auditors.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Qonuni “Axborotlashtirish to‘g‘risida” (O‘RQ-639-son, 17.09.2020).
2. O‘zbekiston Respublikasi Qonuni “Shaxsiy ma’lumotlar to‘g‘risida” (O‘RQ-547-son, 02.07.2019).
3. O‘zbekiston Respublikasi Prezidentining “Axborot xavfsizligini ta’minlash bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-5082-son qarori, 15.04.2021.
4. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash to‘g‘risida”gi PF-6079-son farmoni, 05.10.2020.
5. Xabibullayev X.X. O‘zbekistonda axborot xavfsizligi: hozirgi holat va rivojlanish istiqbollari. – Toshkent: Fan va texnologiya, 2023. – 248 b.
6. Risk Management Framework for Information Systems and Organizations (NIST SP 800-37 Rev. 2). – 2018.
7. Оперативно-розыскная деятельность в сфере информационной безопасности: учебное пособие. – М.: Юнити-Дана, 2022.
8. Кибербезопасность: национальный и международный опыт. – Под ред. А.В. Манойло. – Москва: Горячая линия – Телеком, 2023.
9. Axborot xavfsizligi va kiberxavfsizlik: o‘quv qo‘llanma / A. Abdirashidov, Sh. Sattorov. – Toshkent: TATU nashriyoti, 2024. – 312 b.
10. O‘zbekiston Respublikasi Markaziy bankining “Banklarda axborot xavfsizligini ta’minlash tartibi to‘g‘risida”gi 32/4-son nizomi, 2022.
11. “Kritik axborot infratuzilmasi ob’ektlarini himoyalash talablari” (VM 2023-yil 12-son qarori).
12. Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. 2024-yil axborot xavfsizligi holati bo‘yicha yillik hisobot. – Toshkent, 2025.

References

1. Law of the Republic of Uzbekistan “On Informatization” (No. ZRU-639, 17.09.2020).

2. Law of the Republic of Uzbekistan “On Personal Data” (No. ZRU-547, 02.07.2019).
3. Presidential Decree of the Republic of Uzbekistan No. PQ-5082 “On additional measures to ensure information security” dated 15.04.2021.
4. Presidential Decree of the Republic of Uzbekistan No. PF-6079 “On approval of the Digital Uzbekistan-2030 strategy” dated 05.10.2020.
5. Khabibullayev Kh.Kh. Information security in Uzbekistan: current state and development prospects. – Tashkent: Science and Technology, 2023. – 248 p.
6. Risk Management Framework for Information Systems and Organizations (NIST SP 800-37 Rev. 2). – 2018.
7. Operational-search activity in the sphere of information security: textbook. – Moscow: Unity-Dana, 2022.
8. Cybersecurity: national and international experience / ed. by A.V. Manoilo. – Moscow: Hot Line – Telecom, 2023.
9. Information security and cybersecurity: textbook / A. Abdirashidov, Sh. Sattorov. – Tashkent: TATU Publishing House, 2024. – 312 p.
10. Regulation of the Central Bank of the Republic of Uzbekistan No. 32/4 “On the procedure for ensuring information security in banks”, 2022.
11. “Requirements for protection of critical information infrastructure objects” (Resolution of the Cabinet of Ministers No. 12 of 2023).
12. Ministry of Digital Technologies. Annual report on the state of information security for 2024. – Tashkent, 2025.