ГОСУДАРСТВЕННАЯ ПОЛИТИКА МИНИСТЕРСТВА ЦИФРОВЫХ ТЕХНОЛОГИЙ В ОБЛАСТИ РАЗВИТИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ И ХОСТИНГА ДАННЫХ

ПОЛИТИКА Министерства цифровых технологий Республики Узбекистан О подходах к размещению, хранению и обработке государственных данных в облачных инфраструктурах (облачных вычислительных средах)

I. Введение и назначение документа

Настоящая Политика устанавливает принципы, нормы и механизмы размещения, хранения, обработки и управления государственными данными в облачных вычислительных средах, включая государственные и частные облачные платформы, действующие на территории Республики Узбекистан. Она служит руководством для государственных органов при переходе к цифровым формам работы и отражает стремление страны обеспечить безопасность, эффективность и прозрачность в управлении данными.

Документ направлен на создание устойчивой цифровой экосистемы, в которой облачные решения играют ключевую роль. Применение данной Политики позволит достичь баланса между инновационным развитием, защитой национальных интересов и удовлетворением нужд общества в современных цифровых услугах. Также предусматривается последовательный переход от традиционных моделей хранения информации к гибким и масштабируемым облачным платформам, соответствующим принципам цифрового суверенитета.

II. Цели и задачи политики

Целью настоящей Политики является определение единого подхода к использованию облачных технологий в государственном секторе с приоритетом безопасности, эффективности и прозрачности. Облачные технологии обеспечивают централизованное управление информационными ресурсами, снижение издержек и повышение гибкости процессов.

Задачи включают: – стимулирование использования облачных решений в органах государственного управления; – разработку нормативной базы для обеспечения устойчивости и защиты данных; – развитие Национальной облачной платформы как ядра цифровой инфраструктуры страны; – обеспечение совместимости и интеграции с действующими информационными системами; – повышение цифровой грамотности государственных служащих.

Кроме того, среди задач можно выделить создание унифицированных стандартов взаимодействия между органами власти и частными провайдерами, разработку шаблонных соглашений о сотрудничестве, а также внедрение гибких моделей масштабирования облачных мощностей в зависимости от потребностей государственного сектора.

Политика выступает основой для долгосрочной цифровизации, охватывающей все уровни государственного управления – от министерств до местных органов власти. Также особое внимание уделяется формированию среды доверия среди населения, предпринимателей и других заинтересованных сторон.

III. Классификация данных и режимы хранения

Все данные, обрабатываемые государственными органами, классифицируются в зависимости от их чувствительности. Это необходимо для определения уровня защиты и условий хранения. Введение четкой системы классификации обеспечивает соблюдение принципов защиты персональных данных и государственной тайны.

Категории: – Конфиденциальные данные — информация, подлежащая защите в соответствии с законом о государственной тайне; – Служебные данные — данные ограниченного доступа, представляющие внутреннюю операционную информацию; – Публичные данные — информация, доступная широкому кругу пользователей, включая открытые данные.

Только публичные данные могут размещаться в зарубежных облачных сервисах, при этом резервная копия должна находиться в инфраструктуре Республики Узбекистан. Для конфиденциальных и служебных данных допустимо исключительно локальное размещение с применением сертифицированных систем защиты информации.

Дополнительно следует предусмотреть механизмы периодической ревизии классификации данных. Информационные системы должны обладать встроенной функцией автоматического отслеживания перемещения чувствительных данных и блокировки их выгрузки в неавторизованные облачные среды. Также необходимо предусмотреть автоматическое шифрование данных в момент их перемещения или передачи.

IV. Инфраструктура облачных решений и требования к провайдерам

Ключевым компонентом внедрения облачных решений является создание Национальной облачной платформы. Она включает распределенные центры обработки данных, систему резервного хранения, а также платформу управления виртуальными ресурсами.

Поставщики услуг облачного хранения обязаны: – иметь юридическую регистрацию в Республике Узбекистан; – соблюдать технические и организационные меры по защите данных; – обеспечить высокую доступность сервисов (от 99,9%); – предоставлять механизмы шифрования и резервного копирования; – гарантировать возможность быстрого возврата данных (data portability); – проходить обязательную сертификацию и инспекционный контроль.

Провайдеры обязаны поддерживать журнал событий, хранить метаданные по действиям пользователей и предоставлять отчеты по запросу уполномоченных государственных органов. Обязательным условием является внедрение процедур восстановления после сбоев и дублирование критических компонентов в нескольких географически распределенных узлах.

Министерство цифровых технологий ведет единый реестр аккредитованных поставщиков облачных услуг и осуществляет контроль их соответствия требованиям.

V. Механизмы безопасности и защиты информации

Политика базируется на принципах превентивной безопасности. Каждый облачный проект обязан учитывать потенциальные угрозы и включать меры по их нейтрализации. Государственные органы обязаны внедрять стандарты, обеспечивающие системный подход к управлению безопасностью информации.

Применяются следующие меры: – многофакторная аутентификация доступа; – шифрование данных при передаче и хранении; – контроль действий пользователей с ведением логов; – регулярное проведение аудитов и тестирования на проникновение; – разработка и тестирование планов реагирования на инциденты.

Органы обязаны оперативно реагировать на нарушения, используя механизмы централизованного реагирования на инциденты (CSIRT) и электронные системы оповещения.

Дополнительно предусматривается внедрение системы оценки угроз и раннего оповещения, а также механизма независимого внешнего аудита безопасности с участием профильных экспертов.

VI. Подход к мониторингу, отчетности и управлению эффективностью

Для обеспечения контроля за реализацией настоящей Политики Министерство цифровых технологий внедряет централизованную электронную платформу мониторинга. Через нее осуществляется сбор статистики по использованию облачных ресурсов всеми государственными структурами.

Метрики мониторинга: – объем размещенных данных по категориям; – количество задействованных облачных решений и провайдеров; – уровень удовлетворенности пользователей; – количество выявленных инцидентов безопасности; – экономическая эффективность (снижение затрат, прирост эффективности).

Также включается анализ энергоэффективности центров обработки данных, объемов потребления ресурсов и экологического следа. Это необходимо для соответствия устойчивым практикам в ИКТ и учета экологической составляющей цифровизации.

Министерство ежегодно формирует аналитический отчет, содержащий не только статистику, но и рекомендации по совершенствованию политики, примеры лучших практик и аналитический обзор динамики перехода к облачным решениям.

VII. Финансирование, стимулирование и кадровая поддержка

Государство выделяет средства на развитие облачной инфраструктуры в рамках национальных программ цифровизации. Финансирование осуществляется за счет: –

государственного бюджета; – целевых фондов развития ИКТ; – партнерств с частным сектором (ГЧП); – международной технической помощи.

Стимулы включают: – предоставление грантов на пилотные проекты; – компенсации затрат на миграцию в облачные среды; – субсидии на использование отечественных дата-центров.

Дополнительно предусматриваются налоговые льготы для предприятий, обеспечивающих внедрение облачных решений для нужд государства, а также инвестиционные преференции при создании совместных кластеров.

Для подготовки квалифицированных кадров внедряются: – специализированные курсы и программы повышения квалификации; – аттестация государственных ИТ-специалистов; – национальный резерв экспертов по облачным технологиям.

Также инициируются исследования в области применения облачных технологий в государственном секторе с участием научных и образовательных учреждений страны.

VIII. Заключительные положения

Настоящая Политика вступает в силу с момента утверждения и подлежит пересмотру не реже одного раза в три года. Государственные органы в течение 12 месяцев обязаны провести аудит своих информационных систем и подготовить план по переходу на облачные решения в соответствии с положениями настоящей Политики.

Министерство цифровых технологий оставляет за собой право давать разъяснения по вопросам применения, проводить плановые проверки и внедрять цифровые инструменты для автоматизации контроля.

Применение политики является обязательным условием для финансирования цифровых проектов и подключения к Единой системе межведомственного электронного взаимодействия.

Таким образом, настоящая Политика представляет собой основу для системного и безопасного внедрения облачных технологий в государственном секторе, способствует формированию суверенной цифровой среды и цифровой устойчивости страны в условиях стремительного технологического развития.

STATE POLICY OF THE MINISTRY OF DIGITAL TECHNOLOGIES ON THE DEVELOPMENT OF CLOUD TECHNOLOGIES AND DATA HOSTING

POLICY of the Ministry of Digital Technologies of the Republic of Uzbekistan on Approaches to the Placement, Storage, and Processing of State Data in Cloud Infrastructures (Cloud Computing Environments)

I. Introduction and Purpose of the Document

This Policy establishes the principles, norms, and mechanisms for the placement, storage, processing, and management of state data in cloud computing environments, including both state and private cloud platforms operating within the Republic of Uzbekistan. It serves as a guide for government agencies transitioning to digital workflows and reflects the country's commitment to ensuring the security, efficiency, and transparency of data management.

The document aims to create a sustainable digital ecosystem where cloud solutions play a key role. The application of this Policy will achieve a balance between innovative development, the protection of national interests, and the fulfillment of societal needs for modern digital services. It also envisions a gradual transition from traditional information storage models to flexible and scalable cloud platforms aligned with the principles of digital sovereignty.

II. Objectives and Tasks of the Policy

The purpose of this Policy is to define a unified approach to the use of cloud technologies in the public sector, with a priority on security, efficiency, and transparency. Cloud technologies enable centralized management of information resources, cost reduction, and increased process flexibility.

Tasks include: Promoting the use of cloud solutions in government agencies; Developing a regulatory framework to ensure data stability and protection; Developing the National Cloud Platform as the core of the country's digital infrastructure; Ensuring compatibility and integration with existing information systems; Enhancing the digital literacy of public servants.

Additionally, tasks include establishing unified interaction standards between government bodies and private providers, developing template cooperation agreements, and implementing flexible cloud capacity scaling models based on the needs of the public sector.

The Policy serves as the foundation for long-term digitization, covering all levels of government—from ministries to local authorities. It also places special emphasis on building a trust environment among the public, entrepreneurs, and other stakeholders.

III. Classification of Data and Storage Modes

All data processed by government agencies is classified based on its sensitivity, which is necessary to determine the level of protection and storage conditions. A clear classification system ensures compliance with principles for protecting personal data and state secrets.

Categories:

- **Confidential Data** — information requiring protection under the law on state secrets;
- **Service Data** — restricted-access data representing internal operational information;
- **Public Data** — information accessible to a wide range of users, including open data.

Only public data may be hosted on foreign cloud services, provided a backup copy is maintained within the infrastructure of the Republic of Uzbekistan. For confidential and service data, only local placement with certified information protection systems is permitted.

Additional mechanisms for periodic data classification reviews should be established. Information systems must include a built-in function for automatically tracking the movement of sensitive data and blocking its upload to unauthorized cloud environments. Automatic data encryption during transfer or transmission is also required.

IV. Cloud Solution Infrastructure and Provider Requirements

A key component of implementing cloud solutions is the creation of the National Cloud Platform, which includes distributed data processing centers, a backup storage system, and a platform for managing virtual resources.

Cloud service providers are required to: Be legally registered in the Republic of Uzbekistan; Comply with technical and organizational data protection measures; Ensure high service availability (99.9% uptime); Provide encryption and backup mechanisms; Guarantee data portability (quick data return); Undergo mandatory certification and inspection control.

Providers must maintain an event log, store metadata on user actions, and provide reports upon request by authorized government agencies. A mandatory condition is the implementation of failure recovery procedures and duplication of critical components across multiple geographically distributed nodes.

The Ministry of Digital Technologies maintains a unified registry of accredited cloud service providers and monitors their compliance with requirements.

V. Security Mechanisms and Information Protection

The Policy is based on the principles of preventive security. Every cloud project must account for potential threats and include measures to neutralize them. Government agencies are required to implement standards ensuring a systematic approach to information security management.

The following measures are applied: Multi-factor authentication for access; Data encryption during transmission and storage; User action monitoring with log maintenance; Regular audits and penetration testing; Development and testing of incident response plans.

Agencies must respond promptly to violations using centralized incident response mechanisms (CSIRT) and electronic notification systems.

Additionally, a threat assessment and early warning system, as well as an independent external security audit mechanism involving specialized experts, are to be introduced.

VI. Approach to Monitoring, Reporting, and Efficiency Management

To ensure oversight of the Policy’s implementation, the Ministry of Digital Technologies introduces a centralized electronic monitoring platform. This platform collects statistics on the use of cloud resources by all government structures.

Monitoring metrics include: Volume of data placed by category; Number of deployed cloud solutions and providers; User satisfaction level; Number of identified security incidents; Economic efficiency (cost reduction, efficiency gains).

The analysis also covers the energy efficiency of data processing centers, resource consumption volumes, and environmental footprint. This is necessary to align with sustainable ICT practices and account for the environmental aspect of digitization.

The Ministry prepares an annual analytical report containing not only statistics but also recommendations for policy improvement, best practice examples, and an analytical overview of the transition to cloud solutions.

VII. Financing, Incentives, and Workforce Support

The state allocates funds for cloud infrastructure development under national digitization programs. Funding is provided through: The state budget; Targeted ICT development funds; Public-private partnerships (PPP); International technical assistance.

Incentives include: Grants for pilot projects; Reimbursement of migration costs to cloud environments; Subsidies for using domestic data centers.

Additional tax benefits are provided for enterprises implementing cloud solutions for state needs, along with investment preferences for creating joint clusters.

To train qualified personnel, the following are introduced: Specialized courses and professional development programs; Certification of state IT specialists; A national reserve of cloud technology experts.

Research initiatives on the application of cloud technologies in the public sector, involving scientific and educational institutions, are also launched.

VIII. Final Provisions

This Policy takes effect upon approval and is subject to review at least once every three years. Government agencies are required to conduct an audit of their information systems within 12 months and prepare a plan for transitioning to cloud solutions in accordance with this Policy.

The Ministry of Digital Technologies reserves the right to provide clarifications on its application, conduct scheduled inspections, and implement digital tools for automated control. Compliance with the Policy is a mandatory condition for funding digital projects and connecting to the Unified Interagency Electronic Interaction System.

Thus, this Policy serves as the foundation for the systematic and secure implementation of cloud technologies in the public sector, contributing to the formation of a sovereign digital environment and the country’s digital resilience amid rapid technological development.

RAQAMLI TEXNOLOGIYALAR VAZIRLIGINING BULUT TEXNOLOGIYALARI VA MA’LUMOT XOSTINGINI RIVOJLANTIRISH BO‘YICHA DAVLAT SIYOSATI

O‘zbekiston Respublikasi Raqamli Texnologiyalar Vazirligining Bulut Hisoblash Muhitlarida Davlat Ma’lumotlarini Joylashtirish, Saqlash va Qayta Ishlov Berkishga oid Yondashuvlar to‘g‘risidagi SIYOSATI

I. Hujjatga kirish va maqsadi

Ushbu Siyosat O‘zbekiston Respublikasi hududida faoliyat yurituvchi davlat va xususiy bulut platformalarini o‘z ichiga olgan bulut hisoblash muhitlarida davlat ma’lumotlarini joylashtirish, saqlash, qayta ishlash va boshqarish bo‘yicha tamoyillar, me’yorlar va mexanizmlarni belgilaydi. U davlat idoralarining raqamli ish yuritishga o‘tishida qo‘llanma bo‘lib xizmat qiladi va mamlakatning ma’lumotlarni xavfsiz, samarali va shaffof boshqarishga intilishini aks ettiradi.

Hujjat barqaror raqamli ekotizimni yaratishga qaratilgan bo‘lib, unda bulut yechimlari asosiy rol o‘ynaydi. Ushbu Siyosatning qo‘llanilishi innovatsion rivojlanish, milliy manfaatlar himoyasi va jamiyatning zamonaviy raqamli xizmatlarga bo‘lgan ehtiyojlarini muvozanatlashga yordam beradi. Shuningdek, an’anaviy ma’lumot saqlash modellardan moslashuvchan va kengaytirilishi mumkin bo‘lgan bulut platformalariga, raqamli suverenitet tamoyillariga mos ravishda bosqichma-bosqich o‘tish nazarda tutilgan.

II. Siyosatning maqsadlari va vazifalari

Ushbu Siyosatning maqsadi davlat sektorida bulut texnologiyalaridan foydalanishda xavfsizlik, samaradorlik va shaffoflikka ustuvorlik berib, yagona yondashuvni aniqlashdan iborat. Bulut texnologiyalari axborot resurslarini markazlashgan boshqarishni, xarajatlarning kamayishini va jarayonlarning moslashuvchanligini ta’minlaydi.

Vazifalar quyidagilarni o‘z ichiga oladi: Davlat boshqaruvi organlarida bulut yechimlaridan foydalanishni rag‘batlantirish; Ma’lumotlar barqarorligi va himoyasini ta’minlash uchun me’yoriy bazani ishlab chiqish; Milliy Bulut Platformasini mamlakat raqamli infratuzilmasining yadrosi sifatida rivojlantirish; Amaldagi axborot tizimlari bilan moslashuvchanlik va integratsiyani ta’minlash; Davlat xizmatchilarining raqamli savodxonligini oshirish.

Shuningdek, hokimiyat organlari va xususiy provayderlar o‘rtasida bir xil standartli o‘zaro ta’sir me’yorlarini yaratish, hamkorlik bo‘yicha namunaviy shartnomalarni ishlab chiqish va davlat sektorining ehtiyojlariga qarab bulut quvvatlarini moslashuvchan kengaytirish modellarni joriy etish vazifalari ham ajratiladi.

Siyosat uzoq muddatli raqamlashtirishning asosi bo‘lib, davlat boshqaruvi barcha darajalarini — vazirliklardan mahalliy hokimiyat organlarigacha qamrab oladi. Shuningdek, aholiga, tadbirkorlarga va boshqa manfaatdor tomonlarga ishonch muhitini shakllantirishga alohida e’tibor qaratiladi.

III. Ma’lumotlar tasnifi va saqlash rejimlari

Davlat organlari tomonidan qayta ishlanadigan barcha ma’lumotlar uning sezuvchanligiga qarab tasniflanadi, bu esa himoya darajasini va saqlash shartlarini aniqlash uchun zarur. Aniq tasnif tizimining joriy etilishi shaxsiy ma’lumotlar va davlat sirini himoya qilish tamoyillariga rioya qilishni ta’minlaydi.

Toifalar:

- **Maxfiy ma’lumotlar** — davlat siriga oid qonunga muvofiq himoya talab qiluvchi ma’lumotlar;
- **Xizmatiy ma’lumotlar** — cheklangan kirish huquqiga ega bo‘lgan ichki operatsion ma’lumotlar;
- **Ommaviy ma’lumotlar** — keng foydalanuvchilar uchun, shu jumladan ochiq ma’lumotlar uchun mavjud bo‘lgan ma’lumotlar.

Faqat ommaviy ma’lumotlar chet el bulut xizmatlariga joylashtirilishi mumkin, lekin zaxira nusxasi O‘zbekiston Respublikasi infratuzilmasida saqlanishi shart. Maxfiy va xizmatiy ma’lumotlar uchun faqat mahalliy joylashtirish, sertifikatlangan axborot himoya tizimlari bilan ishlatilishi ruxsat etiladi.

Bundan tashqari, ma’lumotlar tasnifini davriy qayta ko‘rib chiqish mexanizmlarini joriy etish lozim. Axborot tizimlari sezuvchan ma’lumotlar harakatini avtomatik kuzatish va ularni ruxsat etilmagan bulut muhitlariga yuklashni to‘xtatib qo‘yish funksiyasiga ega bo‘lishi kerak. Shuningdek, ma’lumotlar uzatilishi yoki ko‘chirilishi paytida avtomatik shifrlashni joriy etish zarur.

IV. Bulut yechimlar infratuzilmasi va provayderlarga qo‘yiladigan talablar

Bulut yechimlarni joriy qilishning asosiy komponenti Milliy Bulut Platformasini yaratishdan iborat bo‘lib, u tarqalgan ma’lumotlar qayta ishlash markazlarini, zaxira saqlash tizimini va virtual resurslarni boshqarish platformasini o‘z ichiga oladi.

Bulut xizmat provayderlari quyidagi majburiyatlarga ega: O‘zbekiston Respublikasida yuridik ro‘yxatdan o‘tgan bo‘lish; Ma’lumotlarni himoya qilish bo‘yicha texnik va tashkiliy choralarni bajarish; Xizmatlarni yuqori mavjudlikni ta’minlash (99,9% vaqtda ishlaydiganlik); Shifrlash va zaxira nusxalash mexanizmlarini taqdim etish; Ma’lumotlarni tez qaytarish imkoniyatini (data portability) kafolatlash; Majburiy sertifikatlashtirish va tekshiruv nazoratini o‘tkazish.

Provayderlar voqealar jurnalini yuritish, foydalanuvchi harakatlari bo‘yicha metama’lumotlarni saqlash va vakolatli davlat organlarining so‘roviga binoan hisobotlar taqdim etishlari shart. Majburiy shart sifatida nosozliklarni tiklash protseduralarini joriy etish va tanqidiy komponentlarni bir nechta geografik jihatdan tarqalgan tugunlarda takrorlash zarur.

Raqamli Texnologiyalar Vazirligi akkreditatsiya qilingan bulut xizmat provayderlarining yagona reestrini yuritadi va ularning talablarga mosligini nazorat qiladi.

V. Xavfsizlik mexanizmlari va axborot himoyasi

Siyosat profilaktik xavfsizlik tamoyillariga asoslanadi. Har bir bulut loyihasi potentsial tahdidlarni hisobga olishi va ularni zararsizlantirish choralarni o‘z ichiga olishi kerak. Davlat idoralari axborot xavfsizlik boshqarishiga tizimli yondashuvni ta’minlaydigan standartlarni joriy etishga majbur.

Quyidagi choralar qo‘llaniladi: Kirish uchun ko‘p omilli autentifikatsiya; Ma’lumotlarni uzatish va saqlash paytida shifrlash; Foydalanuvchi harakatlarini nazorat qilish va loglarni yuritish;

Muntazam auditlar va penetratsiya sinovlari o‘tkazish; Hodisa javob proyektlarini ishlab chiqish va sinovdan o‘tkazish.

Idoralar buzilishlarga tezkor javob berishlari kerak, bu uchun markazlashgan hodisa javob mexanizmlari (CSIRT) va elektron ogohlantirish tizimlaridan foydalanish lozim.

Bundan tashqari, tahdidlarni baholash va erta ogohlantirish tizimi, shuningdek, maxsus ekspertlar ishtirokida mustaqil tashqi xavfsizlik auditi mexanizmini joriy etish ko‘zda tutilgan.

VI. Monitoring, hisobot berish va samaradorlik boshqaruvi yondashuvi

Siyosatning amalga oshirilishini nazorat qilish uchun Raqamli Texnologiyalar Vazirligi markazlashgan elektron monitoring platformasini joriy etadi. Ushbu platforma orqali barcha davlat tuzilmalari tomonidan bulut resurslaridan foydalanish bo‘yicha statistika yig‘iladi.

Monitoring ko‘rsatkichlari: Toifalar bo‘yicha joylashtirilgan ma’lumotlar hajmi; Ishlatilgan bulut yechimlari va provayderlar soni; Foydalanuvchilar qoniqish darajasi; Aniqlangan xavfsizlik hodisalari soni; Iqtisodiy samaradorlik (xarajatlarning kamayishi, samaradorlik o‘sishi).

Shuningdek, ma’lumotlarni qayta ishlash markazlarining energiya samaradorligi, resurs iste’mol hajmi va ekologik iz tahlili o‘z ichiga olinadi. Bu ICT sohasidagi barqaror amaliyotlar va raqamlashtirishning ekologik jihatini hisobga olish uchun zarur.

Vazirlik har yili nafaqat statistikani, balki siyosatni takomillashtirish bo‘yicha tavsiyalar, eng yaxshi amaliyot namunalarini va bulut yechimlarga o‘tish dinamikasining analitik ko‘rinishini o‘z ichiga olgan analitik hisobot tayyorlaydi.

VII. Moliyalashtirish, rag‘batlantirish va kadrlar qo‘llab-quvvatlash

Davlat milliy raqamlashtirish dasturlari doirasida bulut infratuzilmasini rivojlantirish uchun mablag‘ ajratadi. Moliyalashtirish quyidagi manbalar orqali amalga oshiriladi: Davlat byudjeti; Maqsadli ICT rivojlanish jamg‘armalari; Xususiy-davlat hamkorligi (PPP); Xalqaro texnik yordam.

Rag‘batlantirish choralari: Pilot loyihalar uchun grantlar berish; Bulut muhitlarga migratsiya xarajatlarini qoplash; Mahalliy ma’lumot markazlaridan foydalanish uchun subsidiyalar.

Bundan tashqari, davlat ehtiyojlari uchun bulut yechimlarni joriy etuvchi korxonalar uchun soliq imtiyozlari va qo‘shma klasterlar tashkil etishda investitsion imtiyozlar nazarda tutilgan. Malakali kadrlar tayyorlash uchun quyidagilar joriy etiladi: Maxsus kurslar va malaka oshirish dasturlari; Davlat IT-mutaxassislarini sertifikatlashtirish; Bulut texnologiyalari bo‘yicha milliy ekspert zaxirasi.

Shuningdek, mamlakat ilmiy va ta’lim muassasalari ishtirokida davlat sektorida bulut texnologiyalarni qo‘llash bo‘yicha tadqiqotlar boshlanadi.

VIII. Yakuniy qoidalar

Ushbu Siyosat tasdiqlangan paytdan kuchga kiradi va uch yilda kamida bir marta qayta koʻrib chiqishga tabiiy. Davlat idoralari 12 oy ichida oʻz axborot tizimlarini audit qilishlari va ushbu Siyosatga muvofiqlikda bulut yechimlarga oʻtish rejasini tayyorlashlari shart.

Raqamli Texnologiyalar Vazirligi qoʻllash boʻyicha tushuntirishlar berish, rejalashtirilgan tekshiruvlarni oʻtkazish va nazoratni avtomatlashtirish uchun raqamli vositalarni joriy etish huquqini oʻzida saqlab qoladi.

Siyosatga rioya qilish raqamli loyihalarni moliyalashtirish va Birlashgan Idoralararo Elektron Oʻzaro Ta’sir Tizimiga ulanishning majburiy sharti hisoblanadi.

Shunday qilib, ushbu Siyosat davlat sektorida bulut texnologiyalarini tizimli va xavfsiz joriy etishning asosi boʻlib, suveren raqamli muhitni shakllantirishga va mamlakatning tezkor texnologik rivojlanish sharoitidagi raqamli barqarorligiga hissa qoʻshadi.