Docrobot

Политика Безопасности для Облачного Программного Обеспечения «Платформа Docrobot»

1. Введение

Целью данной политики является обеспечение безопасности данных и информации пользователей облачного программного обеспечения, предоставляемого на территории Республики Казахстан.

2. Применимость

Данная политика распространяется на всех сотрудников, подрядчиков, поставщиков и других сторон, имеющих доступ к облачным сервисам компании.

3. Общие Принципы Безопасности

3.1 Конфиденциальность

- Гарантия, что данные пользователей защищены от несанкционированного доступа и раскрытия.
- Шифрование данных при передаче с использованием SSL (Secure Sockets Layer).

3.2 Целостность

- Обеспечение, что данные остаются неизменными и точными, если это не разрешено и не санкционировано.
- Внедрение механизмов контроля целостности данных, таких как хеширование и контрольные суммы.

3.3 Доступность

- Гарантия доступности сервисов для авторизованных пользователей в соответствии с установленными параметрами качества услуг.
- Использование резервного копирования и планов восстановления после сбоев.

4. Соответствие Законодательству Республики Казахстан

4.1 Закон «О персональных данных и их защите»

- Соблюдение требований к сбору, обработке, хранению и защите персональных данных, указанных в законе Республики Казахстан № 94-V «О персональных данных и их защите».
- Получение явного согласия пользователей на сбор и обработку их персональных данных.

4.2 Закон «Об информатизации»

- Соблюдение норм и требований, установленных законом Республики Казахстан № 418-V «Об информатизации», включая требования по защите критически важной информационной инфраструктуры.

4.3 Локализация данных

- Обеспечение хранения и обработки персональных данных граждан Республики Казахстан на территории страны, как это требуется законодательством.

5. Технические Меры Безопасности

5.1 Аутентификация и Авторизация

- Использование многофакторной аутентификации (MFA) для доступа к критическим системам.
- Реализация ролевой модели доступа (RBAC), обеспечивающей минимально необходимые права для выполнения задач.

5.2 Мониторинг и Логирование

- Внедрение систем мониторинга и логирования для отслеживания и анализа подозрительной активности.
- Хранение логов в защищенном виде и обеспечение их доступности для аудита.

5.3 Управление Уязвимостями

- Регулярное проведение оценки уязвимостей и тестов на проникновение.
- Оперативное обновление и патчинг программного обеспечения для устранения выявленных уязвимостей.

6. Организационные Меры Безопасности

6.1 Обучение и Осведомленность

- Регулярное проведение тренингов по безопасности для сотрудников и пользователей.
- Разработка и распространение руководств по безопасности и практикам безопасного использования.

6.2 Инцидент-менеджмент

- Создание и поддержание процедур реагирования на инциденты безопасности.
- Оперативное уведомление пользователей и регуляторных органов о значительных инцидентах, связанных с безопасностью данных.

7. Заключение

Эта политика безопасности будет регулярно пересматриваться и обновляться для обеспечения соответствия текущим требованиям и угрозам. Все заинтересованные стороны обязаны следовать данной политике для поддержания высокого уровня безопасности и доверия пользователей.

Docrobot

Security Policy for Cloud Software «Docrobot platform»

1. Introduction

The purpose of this policy is to ensure the security of data and information of users of the cloud software provided in the Republic of Kazakhstan.

2. Applicability

This policy applies to all employees, contractors, suppliers, and other parties who have access to the company's cloud services.

3. General Security Principles

3.1 Confidentiality

- Guarantee that user data is protected from unauthorized access and disclosure.
- Encrypt data in transit using SSL (Secure Sockets Layer).

3.2 Integrity

- Ensure that data remains unchanged and accurate unless authorized and sanctioned.
- Implement data integrity control mechanisms such as hashing and checksums.

3.3 Availability

- Guarantee service availability for authorized users in accordance with established service level agreement.
- Use backup and disaster recovery plans.

4. Compliance with the Legislation of the Republic of Kazakhstan

4.1 Law «On Personal Data and Their Protection»

- Comply with the requirements for the collection, processing, storage, and protection of personal data as specified in the Republic of Kazakhstan Law No. 94-V «On Personal Data and Their Protection».
- Obtain explicit consent from users for the collection and processing of their personal data.

4.2 Law «On Informatization»

- Comply with the norms and requirements established by the Republic of Kazakhstan Law No. 418-V «On Informatization», including requirements for the protection of critical information infrastructure.

4.3 Data Localization

- Ensure the storage and processing of personal data of citizens of the Republic of Kazakhstan within the country's territory, as required by law.

5. Technical Security Measures

5.1 Authentication and Authorization

- Use multi-factor authentication (MFA) for access to critical systems.
- Implement a role-based access control (RBAC) model to ensure the minimal necessary privileges for task execution.

5.2 Monitoring and Logging

- Implement monitoring and logging systems to track and analyze suspicious activity.
- Store logs securely and ensure their availability for auditing purposes.

5.3 Vulnerability Management

- Regularly conduct vulnerability assessments and penetration tests.
- Promptly update and patch software to address identified vulnerabilities.

6. Organizational Security Measures

6.1 Training and Awareness

- Regularly conduct security training for employees and users.
- Develop and distribute security guides and best practice manuals.

6.2 Incident Management

- Create and maintain incident response procedures.
- Promptly notify users and regulatory authorities of significant data security incidents.

7. Conclusion

This security policy will be regularly reviewed and updated to ensure compliance with current requirements and threats. All stakeholders are required to follow this policy to maintain a high level of security and user trust.