Утверждено

Приказом № ____ от «____» _____ 20__ г.

Политика безопасности для поставщиков и партнёров ООО «Unitel»

Ташкент 2025 г.

1. Цель

1.1 Настоящая политика направлена на обеспечение соблюдения стандартов безопасности рекомендации при работе с поставщиками и партнёрами, участвующими в реализации IT проектов, которые требуют доступа к информационным системам, данным и инфраструктуре компании.

1.2 Политика призвана минимизировать риски, связанные с информационной безопасностью, и обеспечить защиту данных компании и её клиентов.

2. Область применения

Политика безопасности для поставщиков и партнёров ООО «Unitel» в области IT проектов, имеющих доступ к информационным системам компании, а также для проектов, в рамках которых обрабатываются, передаются или хранятся конфиденциальные данные и важные для бизнеса данные компании.

3. Основные требования

3.1 Требования к безопасной разработке

3.1.1 Все разработчики, работающие над проектами для компании, должны соблюдать принципы безопасной разработки, включая контроль уязвимостей, анализ исходного кода и тестирование безопасности – SAST\DAST\OSA.

SAST (Static Application Security Testing) — это метод анализа безопасности программного кода на ранних этапах разработки путём статического (без запуска) анализа исходного кода для выявления уязвимостей и ошибок.

DAST (Dynamic Application Security Testing) — это метод тестирования безопасности приложения путём анализа его работы в реальном времени, во время выполнения, для выявления уязвимостей из внешней среды без доступа к исходному коду.

OSA (Open Source Analysis) — это процесс анализа и оценки используемых в проекте открытых компонентов и библиотек на предмет уязвимостей, лицензий и соответствия требованиям безопасности.

3.1.2 Проекты должны разрабатываться с учетом стандартов безопасной разработки, таких как OWASP (Open Web Application Security Project), для обеспечения защиты от основных угроз, включая SQL-инъекции, XSS и другие уязвимости.

OWASP (Open Web Application Security Project) — это открытая международная организация, занимающаяся улучшением безопасности веб-приложений через публикацию рекомендаций, стандартов и инструментов.

SQL-инъекция — это тип уязвимости, при котором злоумышленник вставляет вредоносные SQL-запросы во вводимые данные для получения несанкционированного доступа к базе данных или её изменения.

XSS (Cross-Site Scripting) — это уязвимость веб-приложений, при которой злоумышленник внедряет вредоносный скрипт в веб-страницу, чтобы выполнить его в браузере других пользователей и украсть данные или нарушить работу сайта.

3.1.3 Все изменения в коде должны проходить код-ревью с учетом аспектов безопасности.

3.2 Требования к паролям

Все пользователи и системы, подключенные к инфраструктуре компании, должны использовать сложные пароли, соответствующие корпоративным требованиям.

3.2.1 **OWASP (Open Web Application Security Project)** — это открытая международная организация, занимающаяся улучшением безопасности веб-приложений через публикацию рекомендаций, стандартов и инструментов.

3.2.2 Минимальная длина пароля должна составлять 12 символов, включая комбинацию букв, цифр и специальных символов.

3.2.3 Пароли должны обновляться каждые 180 дней, и повторное использование предыдущих паролей должно быть запрещено.

3.2.4 Аутентификационные данные (пароли, токены) не должны храниться в открытом виде или в коде приложений.

Аутентификационные данные (пароли, токены) — это информация, используемая для подтверждения личности пользователя и получения доступа к системам или данным.

3.3 Управление доступом к инфраструктуре Компании через PAM

3.3.1 Все действия, связанные с доступом к критическим системам и данным, должны осуществляться только через решения по управлению привилегиями (PAM).

PAM (Privileged Access Management) — это система и процессы управления и контроля доступа к учетным записям с повышенными привилегиями для предотвращения несанкционированного использования и повышения безопасности.

3.3.2 Доступ к привилегированным учетным записям должен быть предоставлен только на временной основе для выполнения конкретных задач и строго контролироваться.

3.3.3 Все операции через PAM (Privileged Access Management) должны записываться для последующего аудита.

3.4 Требования по передачи логов в SIEM

SIEM (Security Information and Event Management) — это система сбора, анализа и корреляции данных о безопасности из разных источников для обнаружения и реагирования на инциденты.

3.4.1 Все системы, используемые поставщиками и партнёрами, должны быть настроены на передачу логов в корпоративную систему управления событиями информационной безопасности (SIEM).

3.4.2 Логи должны включать информацию о попытках входа, действиях с повышенными привилегиями, критических изменениях в системе и других значимых событиях.

3.4.3 Логи должны быть защищены от модификации и удаляться только в соответствии с политиками хранения.

3.5 Требования по развертыванию EDR и агентов для обнаружения уязвимостей

3.5.1 Поставщики и партнёры должны поддерживать установку и использование решений для обнаружения угроз и реагирования на инциденты на конечных устройствах (EDR).

EDR (Endpoint Detection and Response) — это технология мониторинга и реагирования на угрозы на конечных устройствах (компьютерах, серверах) для быстрого обнаружения, анализа и устранения атак.

3.5.2 Все рабочие станции и серверы, используемые для доступа к корпоративным данным и системам, должны иметь агенты для обнаружения уязвимостей, которые будут регулярно обновляться и сканировать системы на наличие уязвимостей.

3.5.3 Поставщики обязаны немедленно устранять все выявленные уязвимости в своих системах.

3.5.4 Использование серверов, операционных систем и ПО, которое не поддерживает обновления безопасности запрещено.

ПО (программное обеспечение) — это совокупность программ и данных, предназначенных для выполнения определённых задач на компьютерах и других устройствах.

3.6 Требования по двухфакторной аутентификации (2FA)

3.6.1 Все пользователи, получающие доступ к корпоративным системам, обязаны использовать двухфакторную аутентификацию (2FA).

2FA (двухфакторная аутентификация) — это метод защиты учетной записи, при котором для входа требуется два разных фактора подтверждения личности, например пароль и код из SMS или приложения.

3.6.2 2FA должна быть настроена для всех удалённых подключений и доступа к чувствительным системам.

3.6.3 В качестве методов 2FA рекомендуется использовать OTP, биометрию, аппаратные токены или другие безопасные решения.

OTP (One-Time Password) — одноразовый пароль, действующий только для одной сессии или входа, обычно отправляется по SMS или генерируется в приложении.

Биометрия — метод аутентификации на основе уникальных физических характеристик пользователя, таких как отпечаток пальца, лицо или голос.

Аппаратные токены — физические устройства, генерирующие коды или подтверждающие доступ, используемые как дополнительный фактор безопасности.

3.7 Требования по использованию безопасных протоколов

3.7.1 Для аутентификации, авторизации и передачи данных необходимо использовать только безопасные протоколы, такие как OAuth 2.0, SAML, TLS 1.2 или выше.

OAuth 2.0 — протокол авторизации, позволяющий безопасно предоставлять доступ к ресурсам без передачи паролей.

SAML — стандарт обмена данными аутентификации и авторизации между системами для единого входа (SSO).

TLS 1.2 — протокол защиты данных при передаче по сети, обеспечивающий шифрование и безопасность соединения.

3.7.2 Вся передача данных должна быть зашифрована, а устаревшие и небезопасные протоколы, такие как HTTP и FTP, должны быть отключены.

HTTP (HyperText Transfer Protocol) — протокол передачи данных для загрузки и отображения веб-страниц в интернете.

FTP (File Transfer Protocol) — протокол передачи файлов между компьютерами в сети.

3.7.3 Доступ к API-расшифровать и интеграция с системами компании должны быть защищены с помощью токенов, ключей доступа и других методов, обеспечивающих аутентификацию и авторизацию запросов.

API (Application Programming Interface) — это набор правил и инструментов, который позволяет разным программам взаимодействовать и обмениваться данными между собой.

3.7.4 Решения должны поддерживать интеграцию с Active Directory безопасным протоколам – Kerberos, Ldaps.

Active Directory (AD) — это служба каталогов от Microsoft, используемая для управления пользователями, компьютерами и ресурсами в корпоративной сети, обеспечивая централизованную аутентификацию и контроль доступа.

Kerberos — протокол аутентификации, обеспечивающий безопасное подтверждение личности пользователей в сети через систему билетов.

LDAPS (LDAP) — защищённый протокол для безопасного доступа и управления данными в службах каталогов с использованием шифрования.

3.8 Требования по использованию WAF для веб-сервисов

3.8.1 Все веб-сервисы, которые будут разрабатываться и поддерживаться поставщиками или партнёрами, должны быть защищены при помощи Web Application Firewall (WAF).

WAF (Web Application Firewall) — это система защиты веб-сервисов, фильтрующая и блокирующая вредоносный трафик для предотвращения атак на веб-приложения.

3.8.2 WAF должен быть настроен для обнаружения и блокировки атак, таких как SQL-инъекции, XSS, RFI и других видов угроз, выявленных OWASP.

RFI (Remote File Inclusion) — уязвимость веб-приложения, при которой злоумышленник может подключить и выполнить удалённый файл на сервере, что приводит к компрометации системы.

3.8.3 Конфигурация WAF должна периодически обновляться для защиты от новых уязвимостей, и должна быть протестирована перед развертыванием новых функций или изменений в веб-сервисах.

3.9 Требования к базам данных по шифрованию персональных данных

3.9.1 Все базы данных, содержащие персональные данные или чувствительные данные компании, должны использовать шифрование данных на уровне хранения (at-rest).

Хранение at-rest — это хранение данных в состоянии покоя, то есть когда данные сохранены на носителях и не передаются по сети, требующее защиты от несанкционированного доступа.

3.9.2 Шифрование данных должно быть выполнено с использованием современных криптографических алгоритмов (например, AES-256) вид протокола для защиты данных в случае утечки.

AES-256 — это стандарт симметричного шифрования данных с длиной ключа 256 бит, обеспечивающий высокий уровень защиты информации.

3.9.3 Доступ к ключам шифрования должен быть ограничен и управляться через систему управления ключами (KMS, Key Management System).

KMS (Key Management System) — система управления криптографическими ключами, обеспечивающая их создание, хранение, распределение и контроль доступа для защиты данных.

3.9.4 Персональные данные также должны шифроваться при передаче (in-transit), используя защищенные протоколы (например, TLS 1.2 и выше).

(In-transit) — это данные, которые передаются по сети между устройствами и требуют защиты от перехвата и изменений во время передачи.

3.9.5 Поставщики обязаны проводить регулярные проверки на предмет выполнения требований шифрования и представлять отчеты при необходимости.

4. Ответственность

При составлении Технического задания к закупочным мероприятиям **Менеджеры проектов/заказчики** должны согласовать требования с Отделом информационной безопасности компании в тех проектах, где это применимо. Все необходимые требования должны быть отражены в документации при подаче заявки на проведения Закупочного мероприятия в сторону Службы по Закупкам, Контрактам и Логистики.

Поставщики и партнёры обязаны соблюдать требования настоящей политики и обеспечивать, чтобы их сотрудники и подрядчики выполняли все требования безопасности. При этом пункт выше о включении необходимых требований при старте закупочного мероприятия должно быть исполнено.

Отдел информационной безопасности компании отвечает за мониторинг выполнения политики, проведение аудитов и проверку соблюдения установленных стандартов.

5. Исключения

5.1 В случае, если Поставщики и партнеры Компании предлагают альтернативные способы защиты информационных систем, которые отличаются от способов, предусмотренных настоящей Политикой, такие способы допускаются к применению при одновременном соблюдении следующих условий:

- указанные альтернативные способы обеспечения защиты информационных систем обеспечивают уровень защиты, эквивалентный или превосходящий уровень защиты, предусмотренный настоящей Политикой;
- применение таких альтернативных способов получило предварительное согласование отдела информационной безопасности Компании.

6. Контроль и аудит

6.1 Компания оставляет за собой право проводить периодические аудиты безопасности для проверки выполнения данных требований, согласно внутренним процедурам информационной безопасности, включая ежемесячные сканирования на уязвимости систем и контроля доступов.

7. Нарушения и ответственность

7.1 Поставщики и партнёры обязаны нести ответственность за ущерб, причинённый компании в результате несоблюдения требований безопасности, согласно действующему законодательству Республики Узбекистан.