Approved

by Order No. ____ dated ____ _____ 20__

Security Policy for Suppliers and Partners of Unitel LLC

Tashkent, 2025

1. Purpose

1.1 This Policy is intended to ensure compliance with security standards and recommendations in working with suppliers and partners involved in the implementation of IT projects that require access to the Company's information systems, data, and infrastructure.

1.2 The Policy aims to minimize information security risks and ensure the protection of Company and customer data.

2. Scope of Application

This Security Policy applies to suppliers and partners of Unitel LLC involved in IT projects that require access to the Company's information systems, as well as to projects involving the processing, transmission, or storage of confidential or business-critical Company data.

3. Key Requirements

3.1 Secure Development Requirements

3.1.1 All developers working on Company projects must follow secure development principles, including vulnerability control, source code analysis, and security testing — SAST/DAST/OSA.

SAST (Static Application Security Testing) is a method of analyzing application security early in the development cycle by performing static (non-runtime) analysis of source code to identify vulnerabilities and errors.

DAST (Dynamic Application Security Testing) is a method of testing application security by analyzing it during runtime, without access to the source code, to identify vulnerabilities from an external perspective.

OSA (Open Source Analysis) is the process of analyzing and evaluating open-source components and libraries used in a project for vulnerabilities, license compliance, and security requirements.

3.1.2 Projects must be developed in accordance with secure development standards, such as OWASP (Open Web Application Security Project), to ensure protection against key threats, including SQL injections, XSS, and other vulnerabilities.

OWASP (Open Web Application Security Project) is an open international organization focused on improving the security of web applications through recommendations, standards, and tools.

SQL Injection is a vulnerability where an attacker inserts malicious SQL queries into input fields to gain unauthorized access to or manipulate a database.

XSS (Cross-Site Scripting) is a vulnerability where an attacker injects malicious scripts into web pages that are executed in users' browsers, potentially stealing data or disrupting operations.

3.1.3 All code changes must undergo code review with attention to security aspects.

3.2 Password Requirements

All users and systems connected to the Company's infrastructure must use strong passwords that meet corporate requirements.

3.2.1 **OWASP (Open Web Application Security Project)** is an open international organization focused on improving the security of web applications through the publication of recommendations, standards, and tools.

3.2.2 Passwords must be at least 12 characters long and include a combination of letters, numbers, and special characters.

3.2.3 Passwords must be changed every 180 days, and reuse of previous passwords must be prohibited.

3.2.4 Authentication credentials (passwords, tokens) must not be stored in plain text or within application code.

Authentication credentials (passwords, tokens) refer to information used to verify a user's identity and grant access to systems or data.

3.3 Company’s Infrastructure Access Management via PAM

3.3.1 All actions involving access to critical systems and data must be performed through privileged access management (PAM) solutions.

PAM (Privileged Access Management) refers to systems and processes that manage and monitor access to privileged accounts to prevent unauthorized use and enhance security.

3.3.2 Access to privileged accounts must be granted only temporarily for specific tasks and strictly monitored.

3.3.3 All operations performed through PAM (Privileged Access Management) must be recorded for subsequent audit.

3.4 Log Forwarding to SIEM

SIEM (Security Information and Event Management) is a system for collecting, analyzing, and correlating security data from various sources to detect and respond to incidents.

3.4.1 All systems used by suppliers and partners must be configured to forward logs to the corporate Security Information and Event Management (SIEM) system.

3.4.2 Logs must include information on login attempts, privileged actions, critical system changes, and other significant events.

3.4.3 Logs must be protected from modification and deleted only in accordance with retention policies.

3.5 Requirements on EDR Deployment and Vulnerability Detection Agents

3.5.1 Suppliers and partners must support the deployment and use of endpoint detection and response solutions (EDR).

EDR (Endpoint Detection and Response) is a technology for monitoring and responding to threats on endpoint devices (computers, servers) to quickly detect, analyze, and eliminate attacks.

3.5.2 All workstations and servers used to access Company systems or data must have vulnerability detection agents that are regularly updated and scan systems for known vulnerabilities.

3.5.3 Suppliers must promptly remediate any identified vulnerabilities in their systems.

3.5.4 The use of servers, operating systems, and software that no longer receives security updates is prohibited.

Software refers to programs and data designed to perform specific tasks on computers or other devices.

3.6 Two-Factor Authentication (2FA)

3.6.1 All users accessing Company systems must use two-factor authentication (2FA).

2FA (**two-factor authentication**) is a method of account protection requiring two different identity verification factors, such as a password and an SMS or app-generated code.

3.6.2 2FA must be enabled for all remote connections and access to sensitive systems.

3.6.3 Recommended 2FA methods include OTPs, biometrics, hardware tokens, or other secure solutions.

OTP (One-Time Password) is a one-time password valid for only one login session, typically sent via SMS or generated by an app.

Biometrics refers to authentication based on unique physical characteristics such as fingerprints, facial recognition, or voice.

Hardware tokens are physical devices that generate access codes or authorize access as an additional security factor.

3.7 Secure Protocol Requirements

3.7.1 Only secure protocols such as OAuth 2.0, SAML, and TLS 1.2 or higher must be used for authentication, authorization, and data transmission.

OAuth 2.0 is an authorization protocol that enables secure access to resources without sharing passwords.

SAML is a standard for exchanging authentication and authorization data between systems to enable single sign-on (SSO).

TLS 1.2 is a protocol that ensures data encryption and secure connections during transmission over networks.

3.7.2 All data transmissions must be encrypted, and obsolete or insecure protocols such as HTTP and FTP must be disabled.

HTTP (HyperText Transfer Protocol) is a data transfer protocol used to load and display web pages on the internet.

FTP (File Transfer Protocol) is a protocol for transferring files between computers over a network.

3.7.3 API access and integration with Company systems must be protected using tokens, access keys, or other secure methods that authenticate and authorize requests.

API (Application Programming Interface) is a set of rules and tools that allows different software systems to interact and exchange data.

3.7.4 Solutions must support secure integration with Active Directory using protocols such as Kerberos and LDAPS.

Active Directory (AD) is a Microsoft directory service used for managing users, devices, and resources within a Company network, providing centralized authentication and access control.

Kerberos is an authentication protocol providing secure identity verification using ticket-based systems.

LDAPS (LDAP) is a secure protocol for encrypted access and management of directory services.

3.8 Use of WAF for Web Services

3.8.1 All web services developed and maintained by suppliers or partners must be protected by a Web Application Firewall (WAF).

WAF (Web Application Firewall) is a web services protection system that filters and blocks malicious traffic to protect web applications from attacks.

3.8.2 WAF must be configured to detect and block attacks such as SQL injections, XSS, RFI, and other threats identified by OWASP.

RFI (Remote File Inclusion) is a web application vulnerability where an attacker includes and executes a remote file on a server, potentially compromising the system.

3.8.3 WAF configurations must be updated periodically to protect against new threats and tested before deploying new features or changes in web services.

3.9 Database Encryption for Personal Data

3.9.1 All databases containing personal data or sensitive Company data must implement data encryption at the storage level (at-rest).

At-rest storage refers to data held in a dormant state, i.e., stored on physical media and not currently transmitted over a network. Such data must be protected against unauthorized access.

3.9.2 Data encryption must be implemented using modern cryptographic algorithms (e.g., AES-256) as a means of protecting data in the event of a breach.

AES-256 is a symmetric data encryption standard using a 256-bit key, providing a high level of data protection.

3.9.3 Access to encryption keys must be restricted and managed through a Key Management System (KMS).

KMS (Key Management System) is a system for the creation, storage, distribution, and access control of cryptographic keys to ensure data security.

3.9.4 Personal data must also be encrypted during transmission (in-transit) using secure protocols (such as TLS 1.2 or higher).

In-transit refers to data being transmitted over a network between devices, which must be protected from interception or tampering during transfer.

3.9.5 Suppliers are required to perform regular audits to verify compliance with encryption requirements and provide reports upon request.

4. Responsibilities

When drafting Technical Specifications for procurement activities, **Project Managers/Initiators** must coordinate the relevant security requirements with the Company's Information Security Department, where applicable. All necessary requirements must be documented when submitting a Procurement Request to the Procurement, Contracts and Logistics Department.

Suppliers and partners are obligated to comply with the requirements of this Policy and to ensure that their employees and subcontractors fully adhere to all security requirements. Furthermore, the above-mentioned provision regarding the incorporation of security requirements at the initiation of a procurement activity must be duly fulfilled.

The Information Security Department is responsible for monitoring compliance with this Policy, conducting audits, and verifying adherence to established standards.

5. Exceptions

5.1 If the Company's suppliers or partners propose alternative security mechanisms for information systems differing from those outlined in this Policy, such mechanisms may be approved for use provided that:

- the proposed alternatives provide a security level equivalent to or higher than that required by this Policy;
- prior approval has been obtained from the Company's Information Security Department.

6. Control and Audit

6.1 The Company reserves the right to conduct periodic security audits to verify compliance with these requirements in accordance with internal information security procedures, including monthly vulnerability scans and access reviews.

7. Violations and Liability

7.1 Suppliers and partners are liable for any damages caused to the Company due to non-compliance with the security requirements under the applicable legislation of the Republic of Uzbekistan.