The Tanca Approach to Data Security

Table of Contents

Introduction

Tanca is a human resources management software focused on small and medium-sized businesses in Vietnam and other countries. Our primary focus is to solve deep-seated issues related to shift scheduling, attendance tracking, and payroll calculation. Our solution can be integrated with most attendance machines and artificial intelligence cameras in Vietnam.
Our target customer segment is focused on retail chains, F&B chains, distributors, or manufacturers... We handle complex shift scheduling and attendance tracking issues and lead Vietnam in this segment. We currently have over 2500 customers in Vietnam, and our goal is to grow to 30-40 thousand businesses. We currently have more than 180,000 employees using Tanca's services.

1.SecurityTeam and Functions

As a SaaS service provider, Tanca places the security of user services and data as its highest priority. Tanca has a complete security infrastructure and a user service and data security protection system. Tanca's security team consists of security management and compliance, business security, data security, emergency response, and security tool development teams. Its responsibilities include security assessment of product design, code security review, vulnerability scanning, penetration testing, threat intelligence, intrusion detection, emergency response, data security, security compliance, and more.

2.Compliance and Privacy

Tanca attaches great importance to product compliance, and the Security and Compliance Department is responsible for managing compliance with the highest standards at home and abroad. Tanca has a dedicated privacy team that reviews user privacy protocols, product privacy protection design, and the collection and use of user data to ensure that users' data is used correctly and processed and that users are reasonably transparent.
Tanca actively follows international requirements for product compliance and works with various levels of regulatory agencies to ensure that its products and services meet the requirements.
Tanca has passed ISO 27001 certification, which is a set of industrywide adopted security management system standards. It is regarded as one of the most authoritative and strictest information security system certification standard in the world.

3.Employee Security

Tanca has established security human resource management processes:
• The recruitment of new employees must be approved by the human resource (“HR”)

specialist and the resource requesting department leaders. The recruitment process and results are recorded in the human resource management system;
• Before the new employee is hired, the Human Resources Department must conduct background check subject to the laws and regulations of the country according to the importance of the employee's position, to ensure that the recruitment meets Tanca rules and regulations;
• Newly hired employees are required to sign the employment contract and confidentiality agreement which describe the employee's obligations and responsibilities on information security;
• The Legal Department reviews the legal terms enclosed in the employee confidentiality agreement and third-party confidentiality agreement at least once a year and make updates as needed, and publishes the updated agreements through the internal knowledge platform to ensure that all employees and relevant personnel have access to the latest confidentiality agreements;
• The employee's resignation is required to be initiated by the employee himself or herself or the department leader in the human resource management system, and to be approved by the Human Resources Department, the IT Department and other functional departments before the official resignation;
Tanca has established a comprehensive training and learning system. Newly hired employees are required to participate in trainings on corporate culture, rules and regulations, information security, and reward and punishment mechanisms. Meanwhile, Tanca organizes the following trainings to enhance employees' professional knowledge and skills and information security awareness on an aperiodic basis by multiple ways:
• Information security related trainings, to enhance employees' information security skills;
• Information security activities, to promote information security awareness;
• Preparing materials on security awareness topics and delivering to employees via emails and posters

4.App Security

4.1. Operating Environment Security

Tanca App will stringently test the running environment, including root detection, jailbreak detection, etc. The purpose of screening is to ensure that the client runs in a safe and trusted environment, in case the App is hacked or infected by malware.

4.2. Data Security

Tanca App uses the operating system's security mechanism to isolate the permissions between APPs. Full-link communication between the client and the server is encrypted with HTTPS or WSS

4.3. Security Vulnerability Protection

Tanca has a full-time mobile security vulnerability mining team to conduct security assessment and vulnerability mining for android, iOS, clients, as well as vulnerability detection of the client's third-party components (libraries, SDKs), to root out existing vulnerabilities in applications as much as possible to ensure the security of the client.

5.Network Security

5.1. Network Access Control

Tanca uses Amazon Web Services (AWS) to provide infrastructure services, including server rooms, networks, servers, operating systems, etc., and to provide infrastructure security services. Based on AWS, Tanca enhances its security control in server accessing, and all services must be operated and audited through the bastion machine.
Employees need to be authenticated to access internal resources. After confirming their identity, employees have minimal permissions by default. New permission acquisition needs to be approved and recorded by relevant, responsible personnel. Permissions have an expiration date, and the system automatically reclaims permissions after the expiration date. Employees' online service operations are performed through the bastion machine, and all operational logs are retained for audit use.
All employees outside the corporate network boundary need to access Tanca's internal resources through a VPN connection. Tanca's internal audit and control department will audit the access log, search the records for violations of protocol, and handle corresponding reprimands.

5.2. DDoS and Cyber Attack Defense

Tanca Service provides customers around the world with access to its network through CDN and dynamic acceleration and access to back-end service through AWS's load balancing. When encountering DDoS attacks, attack defense will be carried out through a network cleaning service by Cloudflare for example.

5.3. Network Transmission Encryption

Tanca Service is transmitted via HTTPS and WSS in both internal and external networks all the time, which ensures the security of the transmission process and prevents eavesdropping and tampering.

6.Server Security

Tanca uses cloud servers of AWS to serve its customers.
Amazon provides cloud server security from the physical to the virtualization layer. For details on cloud server security provided by AWS, please see Amazon Cloud Security White Paper:
https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

7.Application Security

7.1. Security Development Process

We strive to control security risks from the source of security breaches. All developers and product managers will receive security training to understand the causes of security vulnerabilities and strengthen coding knowledge.The security team will evaluate third-party libraries and tools used by the product and exploit any vulnerabilities to ensure that there are no vulnerabilities introduced by the supply chain then they works with the product team to conduct a security review of the design and coding.

7.2. User Account Security

The user's access to the Tanca system is authenticated using a email/password or phone with random verification code. Each account can be logged in on 1 device at the same time. The risk control system has anti malicious registration, anti- credential enumeration attack, and other protection functions.

7.3. Vulnerabilities and Emergency Response

The Security team receives and reviews vulnerabilities reported from the outside and assesses their harm and urgency to fix them.
The Security team operates a 24/7 emergency response strategy. When a security incident occurs, the security team will quickly classify the event according to the security emergency plan and initiate an emergency response process to prevent the security incident from expanding.

8.Data Security

Tanca has a complete data life cycle management process with a technical guarantee for each stage of the data life cycle, including generation, storage, usage, transmission, sharing, and destruction.

8.1. Data Transmission

Tanca provides users with data transmission channels that support secure encryption protocols. Data transmission such as message pull, identification authentication, operation instructions is encrypted through HTTPS and a 2048-bit RSA key. Message push uses WSS protocol to protect the transmitted data through encryption.

8.2. Data Storage

Tanca uses the key mechanism to support the encrypted storage of data.
Tanca has developed a comprehensive data classification and management method, and strictly classified and classified the user information collected by the Tanca. Tanca has encrypted sensitive data stored in systems, which can effectively protect user information.

8.3. Data Access

User data access is strictly isolated through permissions. Users cannot access each other's accounts without authorization.
Tanca's employees' access to user data is strictly limited and audited, and employees do not have access to any user data by default. Special access requirements are subject to explicit authorization by the user and a strict internal approval process to obtain temporary access rights, in which permissions are immediately reclaimed after the operation is completed. The login log, operation log, and access permission change log of all servers in Tanca’s online environment are recorded.
Tanca will not disclose a user's information publicly unless Tanca has the user's consent. However, in the event that a user's data is required in accordance with laws and regulations, mandatory administrative enforcement or judicial requirements, Tanca may disclose a user's personal information to regulatory law enforcement or legal authorities in accordance with the type of personal data required and the manner in which disclosure is required. When we receive a disclosure request, as laws and regulations approve it, we will need an issuing of legal documents corresponding to the code. We will only provide data that law enforcement agencies have legal rights to obtain for specific investigation purposes. Subject to laws and regulations, the documents we disclose are protected by encryption measures.

8.4. Data Disposal

When terminating service to a user, a Tanca administrator will delete the user account information and will permanently delete the user's data in compliance with local laws and regulations.
Managers can re-onboarding their employees. When a manager deletes an employee, Tanca de-identifies the data and Docs of the requested account based on the tenant administrator's application.

When Tanca signs a service agreement with the user entity, it states that when the service is terminated, the corresponding data will be disposed of according to the user entity's requirements.
Apart from the users from user entities' tenants, Tanca is also applicable to personal users. When an individual user needs to withdraw his or her account, he or she should contact Tanca, which will provide the Tanca installation package with account withdrawal functionality through the Tanca customer service function. After the installation, the user can apply for account withdrawal on the software and Tanca accordingly de-identifies the data and Docs of the requested account in backend databases.

8.5. Data Security Detection

The login behavior, operational behavior in the Tanca online environment are recorded.

9.PhysicalInfrastructureSecurity

Tanca serves customers in different regions of the world through Amazon Web Service As one of the cloud service providers of Tanca, AWS provides services such as cloud servers. AWS itself operates, manages, and controls all of its hardware and software facilities from the physical layer to the virtualization layer. As the world's leading cloud service provider, Amazon has the industry's top security capabilities to provide users with infrastructure security. For details on the protection of cloud service infrastructure provided by AWS, please refer to the AWS Security White Paper:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

10. Disaster Recovery and Service Continuity

10.1. Backup and Disaster Recover

Tanca has established the Data Backup and Recovery Management Policy to standardize backup strategies, backup data retention, and recovery testing methods, etc. Business databases have regular snapshots and backups.

10.2. Service Continuity Guarantee

The service system access layer is accessed in a high-availability mode and through a public gateway service. The back-end uses multi-instance access to ensure the reliability of the service. Through detailed monitoring, if a traffic burst or fault happens, the degraded operation mode will be used to ensure service availability.
Tanca has developed plans to provide guidelines of emergency response and recovery measures to scenarios that may lead to business disruption. Tanca conducts business impact analysis and risk assessment once a year to identify significant business processes and threats that may cause disruptions to Tanca's business and resources;

defines indicators such as maximum tolerable outage time, recovery time target, and minimum service level, etc.; develops respective response strategies for disruption scenarios of different business lines.

10.3. Emergency Drills

Tanca has a complete emergency drill mechanism and conducts fault drills regularly with participants such as the development team, security team, operation, and maintenance team, etc.

11. Change Management

11.1. Source Code Control

Tanca has developed a strict source code management process, and developers can only access and manage the code warehouse corresponding to their team. The R&D personnel has access to the code warehouse, which belongs to his or her group only. Owner of specific code warehouse is required to be set for each project. If the R&D personnel apply for access to the code warehouse belonging to another team, the application should be submitted in the code warehouse. The code warehouse will automatically grant access to the applicant upon receiving the approval from the applicant's team leader and the owner of the applied code warehouse.

11.2. IT Infrastructure Change

Tanca manages the network access by deploying an Access Control List ("ACL") on the public network boundary. If changes are required to be made to the ACL configuration baseline and the network access control policy, the operation personnel apply to the system workflow platform. An engineer from the System Department will implement the change after evaluating the rationality of the change request. Only authorized engineers from the System Department are granted access to change the network access configurations.

11.3. Monitoring Changes

Internal audit is performed by Tanca team each year to assess the operational effectiveness of Tanca's internal control system, including the controls related to change management. The audit results are summarized in the internal audit report. If any exception is identified, the Internal Audit and Internal Control Department will inform the team in charge to take remediation measures and track the remediation status.