ZKTeco WFM

Corporate Security Policy

Contents

ZKTeco WFM Corporate Security Policy

ZKTeco WFM Corporate Security Policy

Effective Date: 06/01/2024
Version: 4.0
Last Updated: 06/01/2024
Approved By: Jaimin Shah, CEO

---

1. Organizational Security

ZKTeco WFM operates with a well-defined Information Security Management System (ISMS) that aligns with our security objectives, focusing on managing risks and implementing mitigation strategies concerning all interested parties. Our policies ensure the security, availability, processing integrity, and confidentiality of customer data.

Employee Background Checks

All employees undergo a thorough background verification process, conducted by reputable third-party agencies. This includes checks on criminal records, previous employment history, and educational background. Until the background check is successfully completed, employees are not assigned to any tasks that could pose risks to users.

Security Awareness and Training

Each employee signs a confidentiality agreement and an acceptable use policy upon induction. This is followed by comprehensive training covering information security, privacy, and compliance. Employees' understanding is evaluated through regular assessments to identify areas for further training. We conduct continuous education on security practices via internal communications and host internal events to raise security awareness.

Dedicated Security and Privacy Teams

ZKTeco WFM has dedicated security and privacy teams responsible for managing and implementing our security and privacy programs. These teams monitor our defense systems, review security processes, and provide domain-specific guidance to the engineering and operational teams. They also continuously monitor the network for suspicious activities.

Internal Audit and Compliance

We have a dedicated compliance team that ensures all security procedures and policies are aligned with industry standards such as SOC and GDPR. Regular internal audits are conducted, and independent assessments are facilitated by third parties.

2. Endpoint Security

Employee Workstations

All employee workstations are maintained with the latest OS versions and are equipped with antivirus software. These systems are configured according to our security standards, which include encryption for data at rest, strong password policies, and automatic locking when idle. Business mobile devices are enrolled in a Mobile Device Management (MDM) system to ensure compliance with security protocols.

3. Physical Security

At Workplace

ZKTeco WFM controls access to its premises, data centers, and infrastructure using access cards. Different levels of access are granted based on roles, and access logs are maintained to detect anomalies. Visitors, contractors, and vendors are issued limited access cards specific to their purpose for entry.

At Data Centers

Our data centers, hosted by AWS, implement strict physical security protocols. Access to these facilities is limited to authorized personnel and is controlled through multi-factor and biometric authentication. All access is logged and monitored via CCTV.

Monitoring

All entries and exits from business centers and data centers are monitored with CCTV, in accordance with local regulations. Backup footage is available for a predetermined period as required by location.

4. Infrastructure Security

Network Security

We employ firewalls to prevent unauthorized access to our network and use segmentation to protect sensitive data. Testing and development environments are isolated from production systems. Regular reviews and audits are conducted on firewall rules, and any suspicious activities are monitored by our Network Operations Center (NOC).

Network Redundancy

Our infrastructure is designed with redundancy at every level, including distributed architecture, redundant switches, and security gateways to avoid single points of failure. This ensures business continuity in the event of a system failure.

DDoS Protection

We utilize trusted third-party technologies to protect our systems from DDoS attacks. These services include real-time monitoring, rate limiting, and scrubbing to ensure that legitimate traffic remains unaffected while blocking malicious activities.

Intrusion Detection and Prevention

Our intrusion detection system monitors host-based signals on individual devices and network-based signals across the infrastructure. Administrative access logs and privileged commands are tracked continuously. The system uses machine learning algorithms to detect anomalies and trigger security alerts.

5. Data Security

Secure by Design

ZKTeco WFM follows a rigorous Software Development Life Cycle (SDLC), ensuring that every new feature and change is vetted for security compliance. Secure coding practices based on OWASP standards help mitigate vulnerabilities like SQL injection and cross-site scripting.

Encryption

In Transit:

All customer data transmitted across public networks is encrypted using Transport Layer Security (TLS 1.2/1.3) protocols, ensuring that both parties in the connection are authenticated and that data remains confidential.

At Rest:

Sensitive customer data stored in our systems is encrypted using AES-256 encryption. We maintain control over encryption keys through our Key Management Service (KMS), adding an extra layer of security by keeping data encryption keys and master keys physically separated.

6. Identity and Access Control

Single Sign-On (SSO)

We offer Single Sign-On (SSO) to our customers, allowing access to multiple services through a single authentication portal. We support SAML-based SSO for integrating with external identity providers such as LDAP and ADFS.

Multi-Factor Authentication (MFA)

We provide MFA to add an additional layer of security. Users can choose from various authentication methods, such time-based OTP through SMS or E-mail.

7. Operational Security

Logging and Monitoring

ZKTeco WFM employs a comprehensive logging and monitoring system. We capture and analyze event logs, audit logs, and user activity logs to detect anomalies. These logs are securely stored and audited regularly to ensure security and compliance.

Vulnerability Management

Our vulnerability management program includes regular scans using industry-standard tools, automated penetration testing, and manual security reviews. Detected vulnerabilities are prioritized, assigned to owners, and tracked until resolved.

8. Data Retention and Disposal

We retain customer data as long as required by the service agreement. Upon service termination, customer data is deleted from active databases during the next cleanup cycle which normally happens once every quarter. Backup data is securely deleted after three months. Devices storing sensitive information are securely wiped and physically destroyed when decommissioned.

9. Incident Management

Reporting and Response

In the event of a security incident, ZKTeco WFM promptly notifies affected customers and provides any necessary forensic data. A dedicated incident management team ensures incidents are tracked, investigated, and mitigated. Breach notifications are handled according to GDPR guidelines and other applicable data protection laws.

10. Vendor Management

ZKTeco WFM evaluates vendors based on our vendor management policy, ensuring that their security protocols align with our commitments. Regular audits and risk assessments are performed to monitor their adherence to confidentiality, integrity, and availability standards.

11. Customer Security Controls

Customers are encouraged to follow best practices, such as using strong passwords, enabling MFA, and keeping their software updated to prevent unauthorized access.

Conclusion

ZKTeco WFM is committed to protecting customer data and maintaining the highest security standards. For additional information on our security practices or to report any concerns, please contact our security team at [security@zktecowfm.com].

Audit Checklist:

1. **Organizational Security**

- **Information Security Management System (ISMS) Documentation**
  - Policies and procedures governing ISMS, including risk management, mitigation strategies, and customer data security processes.
- **Employee Background Checks**
  - Documentation of background verification reports (criminal records, employment history, educational background) for all employees.
- **Security Awareness and Training Programs**
  - Records of employee confidentiality agreements and acceptable use policies.
  - Security training materials, training schedules, and employee participation records.
  - Results of employee security assessments and plans for additional training if required.
- **Security and Privacy Team Documentation**
  - Roles and responsibilities of the dedicated security and privacy teams.
  - Incident monitoring and response processes implemented by these teams.
- **Internal Audit and Compliance Reports**
  - Reports from internal audits and independent assessments regarding SOC, GDPR, and other industry standards.
  - Details on corrective actions taken post-audit.

2. Endpoint Security

- **Endpoint Configuration Policies**
  - Details on workstation configurations (encryption, antivirus software, password policies).
  - Logs of OS version updates, antivirus updates, and software patching schedules.
  - Mobile Device Management (MDM) system setup and compliance logs for business mobile devices.
  - Documentation of encryption standards used for data at rest.
  - Evidence of employee adherence to strong password policies and automatic workstation locking mechanisms.

3. Physical Security

- **Access Control Logs and Policies**
  - Records of access control systems for ZKTeco WFM premises and data centers (access cards, role-based access levels, and logs).
  - Visitor, contractor, and vendor access logs.
- **Data Center Security Protocols**
  - Documentation of AWS data center security protocols, multi-factor authentication, and biometric access control.
  - Logs of authorized personnel access to data centers and monitoring through CCTV.
- **CCTV Monitoring and Retention Policies**
  - Policies governing CCTV usage, backup footage retention periods, and compliance with local regulations.

4. Infrastructure Security

- **Network Security Policies**
  - Firewall configuration policies and firewall rule review/audit reports.

    - Network segmentation policies between development and production environments.
    - Logs and reports from the Network Operations Center (NOC) on suspicious activities or incidents.
- **Network Redundancy Documentation**
    - Design documentation showing redundancy in network architecture (distributed systems, security gateways, etc.).
    - Reports on business continuity testing and failover processes.
- **DDoS Protection Logs**
    - Documentation of third-party services used for DDoS protection (rate limiting, traffic scrubbing).
    - Logs from real-time monitoring and actions taken to prevent DDoS attacks.
- **Intrusion Detection and Prevention (IDP) Logs**
    - Documentation of the intrusion detection system (IDS) configuration and alerts.
    - Logs of host-based and network-based signal monitoring, anomaly detection, and security alerts.

5. Data Security

- **Secure Software Development Life Cycle (SDLC) Documentation**
    - Evidence of secure coding practices following OWASP standards (vulnerability scanning, reviews for SQL injection, XSS).
    - Audit trails for all new features and security reviews before deployment.
- **Encryption Logs and Policies**
    - Policies governing encryption of data in transit (TLS 1.2/1.3) and at rest (AES-256).
    - Documentation of encryption key management practices (KMS usage and key rotation schedules).
    - Logs verifying customer data encryption during transmission and storage.

6. Identity and Access Control

- **Single Sign-On (SSO) Documentation**
    - SSO configuration and integration logs with external identity providers (LDAP, ADFS).
- **Multi-Factor Authentication (MFA) Records**
    - Logs and documentation of MFA setup (biometrics, OTP, hardware security keys) for employee and customer accounts.
    - Evidence of user adoption of MFA for securing access to systems.

7. Operational Security

- **Logging and Monitoring Systems**
    - Logs and reports from the comprehensive logging and monitoring system (event logs, audit logs, and user activity logs).
    - Audit trails for log reviews and responses to security alerts or anomalies.
- **Vulnerability Management Reports**
    - Reports from vulnerability scanning tools, penetration tests, and manual security reviews.
    - Documentation of detected vulnerabilities and corresponding corrective actions taken (prioritization, tracking, resolution logs).

8. Data Retention and Disposal

- **Data Retention Policies**
  - Policies governing customer data retention timelines based on service agreements.
  - Logs showing the deletion of customer data from active databases and backups (after service termination).
  - Documentation of secure data disposal practices (device wiping, physical destruction of storage media).

9. Incident Management

- **Incident Response Plans and Logs**
  - Incident response playbooks detailing procedures for detecting, managing, and reporting security incidents.
  - Logs from security incidents, forensic analysis, and notifications sent to affected customers.
  - GDPR breach notification processes and compliance reports for security incidents.

10. Vendor Management

- **Vendor Security Assessment Reports**
  - Risk assessments and security audits performed on third-party vendors.
  - Vendor contracts and SLAs ensuring compliance with ZKTeco WFM's confidentiality, integrity, and availability standards.

11. Customer Security Controls

- **Customer Security Guidelines and Best Practices**
  - Documentation provided to customers outlining security best practices (MFA usage, password policies, software updates).
  - Logs verifying customer adherence to recommended security practices.

Conclusion

- **Compliance Reports and Audit Preparedness**
  - All security reports, logs, policies, and evidence gathered in preparation for the external audit, ensuring compliance with industry standards such as SOC, GDPR, and others.

ZKTeco WFM System Development Life Cycle (SDLC) Standards and Policy

1. PURPOSE

The purpose of the Systems Development Life Cycle (SDLC) Standards and Policy is to establish a comprehensive framework for the development and implementation of new software and systems at ZKTeco. This document outlines the minimum required phases, tasks, and considerations necessary to ensure that all systems and software are developed in a structured, secure, and efficient manner.

2. SCOPE

This policy applies to all ZKTeco employees, subsidiaries, and covered individuals (e.g., business partners, vendors, independent contractors) involved in software or systems development activities under the auspices of ZKTeco.

3. SDLC Standards

All systems and software development at ZKTeco and its subsidiaries must adhere to industry best practices as defined by the SSAE-16 audit criteria. The SDLC comprises the following phases, each with specific tasks and considerations:

3.1 System Initiation

- **Definition of Need or Opportunity:** Identify the business need or opportunity.
- **Concept Proposal:** Develop an initial concept or proposal.
- **Feasibility Study:** Conduct a preliminary feasibility analysis.
- **Project Charter:** Formulate a project charter if required.

3.2 System Requirements Analysis

- **Requirement Gathering:** Collect and analyze customer requirements.
- **Functional Requirements Document:** Create a detailed Functional Requirements Document (FRD).
- **System Breakdown:** Decompose the system into discrete modules using diagrams and visual tools.
- **Security Requirements:** Define any security requirements

3.3 System Design

- **Detail Design Document:** Transform requirements into a detailed design document.
- **Functionality Description:** Describe the functions and operations of the system or software in detail.
- **Risk Analysis:** Conduct a risk analysis between the System Requirements and System Design phases.
- **Design Review:** Ensure the design addresses practicality, efficiency, cost, flexibility, and security through a final review.

3.4 System Construction (Procurement)

- **Product Development:** Convert design documents into a final product or solution.

- **Testing:** Perform manual and automated unit/module testing throughout this phase. Consider security during testing.
- **Third-Party Solutions:** Evaluate third-party products as potential solutions. Ensure subsequent phases are followed regardless of development source.

3.5 System Testing and Acceptance

- **Validation:** Confirm that the system meets all functional requirements as defined during the System Requirements Analysis phase.
- **Quality Assurance (QA):** Conduct QA testing with a team separate from development.
- **User Acceptance Testing (UAT):** Have the operations support team perform user acceptance testing.
- **Documentation:** Ensure testing documentation is detailed and matches criteria to specific requirements.
- **Holistic Testing:** Conduct holistic testing of the system and final acceptance testing by the operations team or customer.
- **Security Assessment:** Perform a final security assessment.
- **Problem Resolution:** Address any issues identified during previous phases before implementation.

3.6 System Implementation

- **Production Deployment:** Move the fully tested and user-accepted system from the testing environment to production.
- **Development Tools Removal:** Remove all development and testing tools, code, and access mechanisms before production deployment.
- **User Training:** Conduct necessary user training prior to or during implementation.

3.7 System Maintenance

- **Ongoing Support:** Provide continuous support throughout the system's lifecycle, until decommissioning.
- **Support Structure:** Establish a customer/user support structure and operational support processes.
- **Change Management:** Schedule, communicate, and document any planned changes.
- **Security Testing:** Conduct continuous security penetration testing at regular intervals, and mandatory testing after major changes.

4 SDLC Policy Statement

ZKTeco is committed to adhering to the SDLC standards as outlined above for all systems development projects. This policy applies to ZKTeco and its subsidiaries involved in any form of system or software development.

Additional Requirements:

- **In-House Software Development:** All in-house software must adhere to the ZKTeco SDLC Standards. This includes phases from preliminary analysis to post-implementation maintenance.
- **Environment Separation:** Maintain a clear separation between production, development, and test environments to enhance management and security. Exceptions may apply where licensing restrictions prohibit this separation.
- **Access Restrictions:** Development and QA/test staff must not access production systems unless explicitly required by their job duties.

- **Access Path Management:** Delete or disable any non-formal access paths used during development or testing before production deployment.
- **Documentation and Security:** Maintain and update documentation throughout all development phases. Security considerations must be integrated into all phases of the SDLC.

ZKTeco WFM Disaster Recovery and Backup Policy

1. Introduction

1.1. Purpose
The purpose of the ZKTeco WFM Disaster Recovery and Backup Policy is to establish a comprehensive framework for ensuring business continuity, protecting data integrity, and enabling timely recovery of services in the event of a disaster. This policy is specifically designed for ZKTeco WFM's cloud-based infrastructure, hosted on Amazon Web Services (AWS), and aims to minimize disruptions and safeguard against data loss.

1.2. Scope
This policy applies to all ZKTeco WFM personnel, subsidiaries, and business partners involved in managing, maintaining, or utilizing ZKTeco WFM's cloud-based services. The policy covers disaster recovery strategies, backup procedures, and communication plans to ensure that critical business functions can continue with minimal interruption.

1.3. Statement of Confidentiality
This document contains proprietary information of ZKTeco WFM. Unauthorized disclosure, duplication, or distribution of its content is strictly prohibited. All personnel must adhere to confidentiality agreements regarding the handling of sensitive information contained herein.

2. Policy Overview

2.1. Objective
The objective of this policy is to define the processes and procedures required to ensure that ZKTeco WFM's critical services remain available or can be quickly restored following a disaster. This includes data protection, system recovery, and communication strategies that are aligned with industry best practices.

2.2. Policy Statement
ZKTeco WFM is committed to maintaining the availability, integrity, and confidentiality of its services by implementing a robust disaster recovery and backup strategy. This policy mandates regular testing, continuous improvement, and compliance with all relevant regulatory and legal requirements.

3. Disaster Recovery Strategy

3.1. Cloud-Based Infrastructure
ZKTeco WFM's infrastructure is fully cloud-based, with all systems hosted on AWS. This architecture provides resilience, scalability, and redundancy across multiple AWS regions.

3.1 Redundancy and High Availability
- **3.1.1 Data Redundancy:** Data is replicated across multiple AWS regions to prevent data loss and ensure availability in the event of a regional outage.
- **3.1.2 Multi-Factor Authentication (MFA):** MFA is enforced for access to all critical systems to enhance security.

3.1.3 Multiple Internet Service Providers (ISPs): ZKTeco WFM uses multiple ISPs to ensure continuous connectivity.

3.1.4 Physical and Network Security: Biometric physical security, firewalls, and continuous monitoring are in place to protect against unauthorized access and threats.

3.2 Backup and Recovery

3.2.1 Automated Backups: All data is automatically backed up using AWS backup services. Backups are stored in multiple regions for added resilience.

3.2.2 Disaster Recovery as a Service (DRaaS): AWS provides DRaaS, enabling rapid recovery of systems and data with minimal downtime.

3.2.3 Encryption: All backups are encrypted to ensure the confidentiality and integrity of data.

4 Backup Policy

4.1 Data Backup Schedule

4.1.1 Daily Backups: Full backups of all critical data and systems are performed daily and stored in geographically diverse AWS regions.

4.1.2 Incremental Backups: Incremental backups are performed every six hours to capture changes made since the last full backup.

4.1.3 Retention Policy: Backups are retained for a minimum of 30 days, with specific data retained longer as required by regulatory and business needs.

4.2 Backup Storage

4.2.1 Geographic Diversity: Backups are stored in multiple AWS regions to ensure data is not lost in the event of a regional disaster.

4.2.2 Access Controls: Access to backup data is restricted to authorized personnel only, with strict access controls and logging in place.

4.2.3 Testing of Backups: Backups are regularly tested to ensure they can be restored successfully.

5 Disaster Recovery Procedures

5.1 Incident Identification and Notification

5.1.1 Monitoring: Continuous monitoring of cloud infrastructure is conducted to detect issues. Automated alerts are sent to the Disaster Recovery Team when a potential disaster is detected.

5.1.2 Immediate Actions: The Disaster Recovery Team assesses the situation and activates the disaster recovery plan as necessary.

5.2 Recovery Phases

5.2.1 Phase 1 - Initial Response: Assess the impact and determine the extent of the disaster. Prioritize the recovery of critical systems.

5.2.2 Phase 2 - Data Restoration: Restore data from the most recent backups stored in a different AWS region.

5.2.3 Phase 3 - System Recovery: Recover and test critical systems to ensure full functionality and security.

5.2.4 Phase 4 - Service Restoration: Bring all services back online, prioritizing those critical to business operations.

6 Continuous Operations

6.1 Remote Work Capability: All employees have secure VPN access to cloud resources, enabling them to work remotely during a disaster.

6.2 Third-Party Services: Continuity of third-party services (e.g., Microsoft 365, Atlassian, Zoho) is ensured through their respective cloud providers.

7 Recovery Team and Responsibilities

7.1 Recovery Team

7.1.1 Disaster Recovery Team: The Disaster Recovery Team is responsible for executing the disaster recovery plan. Key roles include:

7.1.2 DR Coordinator: Leads the disaster recovery efforts and coordinates all activities.

7.1.3 Cloud Infrastructure Lead: Manages the recovery of cloud-based systems and data.

7.1.4 Security Lead: Ensures the security of recovered systems and data.

7.1.5 Communications Lead: Manages internal and external communications during and after the disaster.

7.2 Responsibilities

7.2.1 DR Coordinator: Activates the disaster recovery plan, coordinates efforts, and communicates with executive management.

7.2.2 Cloud Infrastructure Lead: Restores data and systems from backups and ensures their integrity.

7.2.3 Security Lead: Monitors for ongoing threats and secures all systems during the recovery process.

7.2.4 Communications Lead: Provides updates to stakeholders, including employees, customers, and the media.

8 Communication Plan

8.1 Internal Communication

8.1.1 Alert System: Use cloud-based communication tools (e.g., Microsoft Teams, email) to notify the Disaster Recovery Team and employees.

8.1.2 Regular Updates: Provide frequent updates on the status of recovery efforts via email and the company intranet.

8.2 External Communication

8.2.1 Customer Notifications: Inform customers about any service disruptions and expected recovery times.

8.2.2 Public Relations: The designated spokesperson handles all media inquiries to ensure consistent messaging.

9 Testing and Maintenance

9.1 Testing Schedule

9.1.1 Quarterly Testing: Conduct quarterly disaster recovery tests, including data restoration and service recovery simulations.

9.1.2 Annual Full-Scale Test: Perform a full-scale disaster recovery test annually to ensure the plan's effectiveness.

9.2 Continuous Improvement

9.2.1 Plan Review: Review and update the disaster recovery and backup policy annually or after any significant infrastructure changes.

9.2.2 Documentation: Keep all recovery procedures and contact information up to date.

10 Appendices

10.1 Contact Information: A list of contact details for all key personnel, including the Disaster Recovery Team, service providers, and emergency contacts.

10.2 **Recovery Checklists:** Detailed checklists for each phase of the disaster recovery process.

10.3 **External Documents:** References to any external documents, such as AWS recovery documentation and vendor agreements.

ZKTeco Data Processing Agreement

Last Modified: January 2024

This Data Processing Agreement ("DPA") outlines the terms governing the Processing of Personal Data by ZKTeco on behalf of the Customer in connection with the ZKTeco CirrusDCS Master Services Agreement (the "Agreement"). This DPA is an integral part of the Agreement and is effective upon incorporation into the Agreement, which may occur via an Order or an amendment. In case of conflict with the Agreement, this DPA will take precedence.

ZKTeco will provide 30 days' written notice for any updates to this DPA.

---

1. Definitions

1.1. **California Personal Information** – Personal Data subject to protection under the California Consumer Privacy Act (CCPA).

1.2. **CCPA** – California Civil Code Sec. 1798.100 et seq., as amended by the California Privacy Rights Act (CPRA).

1.3. **Consumer, Business, Sell, Service Provider** – Have the same meanings as set forth in the CCPA.

1.4. **Controller** – A person or entity that determines the purposes and means of Processing Personal Data.

1.5. **Data Privacy Framework** – The EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework.

1.6. **Data Protection Laws** – All applicable global laws regulating data protection and privacy, including European Data Protection Laws, the CCPA, and other applicable laws in regions like Australia, Singapore, and Japan.

1.7. **Data Subject** – The individual to whom Personal Data relates.

1.8. **European Data** – Personal Data subject to protection under European Data Protection Laws.

1.9. **European Data Protection Laws** – Data protection laws in Europe, including the GDPR, UK GDPR, and Swiss DPA.

1.10. **Instructions** – Documented directions from the Controller to the Processor regarding Personal Data Processing.

1.11. **Permitted Affiliates** – Affiliates of the Customer allowed to use ZKTeco services and who qualify as Controllers of Personal Data.

1.12. **Personal Data** – Any information relating to an identified or identifiable individual.

1.13. **Personal Data Breach** – A security breach leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.14. **Processing** – Any operation performed on Personal Data, such as collection, storage, use, disclosure, or deletion.

1.15. **Processor** – ZKTeco or any entity Processing Personal Data on behalf of the Controller.

1.16. **Standard Contractual Clauses** – The standard clauses adopted by the European Commission for cross-border transfers of Personal Data.

1.17. **Sub-Processor** – A third-party entity engaged by ZKTeco to assist in Processing Personal Data.

1.18. **UK Addendum** – The UK-specific addendum for data transfers under the Data Protection Act 2018.

---

2. Customer Responsibilities

2.1. **Compliance with Laws**
Customer is responsible for complying with all applicable Data Protection Laws, including obtaining necessary consents for Personal Data Processing. The Customer must ensure that:

- The Personal Data it provides to ZKTeco is accurate, lawful, and compliant with all relevant privacy regulations.
- The Instructions issued to ZKTeco for Processing are legal and comply with Data Protection Laws.
- Appropriate consents and authorizations for Personal Data, particularly for marketing, are obtained.

2.2. **Controller Instructions**
The Agreement, together with this DPA, constitutes the Customer's complete Instructions to ZKTeco regarding the Processing of Personal Data. The Customer may issue additional lawful Instructions during the term of the subscription service.

2.3. **Security**
Customer is responsible for determining if ZKTeco's security measures are sufficient for its compliance obligations under Data Protection Laws. The Customer is also responsible for securing data in transit to and from ZKTeco's services.

---

3. ZKTeco Obligations

3.1. **Compliance with Instructions**
ZKTeco will only Process Personal Data as directed by the Customer’s lawful Instructions and is not responsible for compliance with industry-specific Data Protection Laws that do not apply to ZKTeco.

3.2. **Conflict of Laws**
If ZKTeco is legally required to Process Personal Data contrary to the Customer's Instructions, it will notify the Customer unless prohibited by law.

3.3. **Security**
ZKTeco will implement and maintain appropriate technical and organizational measures to protect Personal Data from breaches, as described in Annex 2 (Security Measures).

3.4. **Confidentiality**
ZKTeco will ensure that personnel authorized to Process Personal Data are bound by confidentiality obligations.

3.5. **Personal Data Breaches**
In the event of a breach, ZKTeco will notify the Customer without undue delay and provide necessary assistance to enable the Customer to meet regulatory obligations for breach notifications.

3.6. **Data Deletion or Return**
Upon termination or expiration of the Agreement, ZKTeco will delete or return all Personal Data per the CirrusDCS Services Privacy Policy.

---

4. Data Subject Requests

4.1. ZKTeco provides tools for Customers to retrieve, correct, or delete Personal Data in compliance with Data Protection Laws. If additional assistance is needed, ZKTeco will support the Customer, and any costs incurred will be reimbursed.

4.2. If ZKTeco receives a Data Subject Request directly, it will inform the Customer and advise the Data Subject to contact the Customer directly.

---

5. Sub-Processors

5.1. ZKTeco may engage Sub-Processors to assist in providing the Services.

5.2. Customers will be notified of any new Sub-Processors 30 days in advance and may object on reasonable grounds.

5.3. ZKTeco remains responsible for Sub-Processors' compliance with the DPA and will ensure Sub-Processors offer the same level of data protection.

---

6. Data Transfers

ZKTeco may Process Personal Data globally to provide the Services. Transfers of Personal Data will be done in compliance with applicable Data Protection Laws, including the use of appropriate safeguards like the Standard Contractual Clauses.

---

7. Demonstration of Compliance

ZKTeco will provide all necessary information to demonstrate compliance with this DPA, including allowing audits. ZKTeco uses Amazon Web Services (AWS), which maintains SOC 2, NIST, ISO,

and FedRAMP certifications. ZKTeco will also provide summaries of its penetration testing results upon request.

---

8. Additional Provisions for European Data

8.1. This section applies only to European Data.

8.2. ZKTeco acts as the Processor for European Data, and the Customer is the Controller.

8.3. If Customer Instructions violate European Data Protection Laws, ZKTeco will inform the Customer.

8.4. Sub-Processor agreements and any necessary Standard Contractual Clauses will be provided on a confidential basis.

8.5. ZKTeco will assist the Customer with data protection impact assessments and regulatory consultations if required.

8.6. **Transfer Mechanisms for Data Transfers**
ZKTeco will comply with all applicable transfer mechanisms, such as the Data Privacy Framework and Standard Contractual Clauses, for transferring European Data outside the European Economic Area (EEA).

---

9. Additional Provisions for California Personal Information

9.1. This section applies only to California Personal Information.

9.2. ZKTeco acts as a Service Provider under the CCPA.

9.3. ZKTeco will not Sell or Share California Personal Information and will Process it only for the purposes specified in the Agreement.

9.4. ZKTeco certifies compliance with the CCPA's requirements for Service Providers.

---

10. General Provisions

10.1. **Amendments**
ZKTeco may update this DPA as needed and will notify the Customer 30 days in advance.

10.2. **Severability**
If any provision of this DPA is deemed invalid, the remainder of the DPA will remain in full force.

10.3. **Limitation of Liability**
Liability under this DPA is subject to the limitations set out in the Agreement.

10.4. **Governing Law**
This DPA is governed by the same laws as the Agreement unless otherwise required by Data Protection Laws.

---

11. Parties to this DPA

11.1. **Permitted Affiliates**
The Customer enters this DPA on behalf of its Permitted Affiliates, binding them to the terms of the Agreement and DPA.

11.2. **Authorization**
The Customer entity signing the Agreement represents that it is authorized to enter into the DPA on behalf of its Affiliates.

ZKTeco WFM Vendor Management and Compliance Policy

1. Purpose

The purpose of this policy is to establish a framework for managing relationships with vendors and ensuring compliance with all applicable legal, regulatory, and company-specific requirements. This policy is designed to protect the interests of ZKTeco WFM by ensuring that vendors meet our standards for security, data protection, performance, and ethical conduct.

2. Scope

This policy applies to all vendors who provide products or services to ZKTeco WFM. This includes, but is not limited to, suppliers, subcontractors, service providers, and any other third-party entities engaged in business with ZKTeco WFM.

3. Vendor Selection

- **Due Diligence:** Before entering into a relationship with any vendor, ZKTeco WFM will conduct thorough due diligence. This includes an assessment of the vendor's financial stability, reputation, business practices, and compliance with relevant laws and regulations.
- **Risk Assessment:** A risk assessment will be performed to evaluate the potential risks associated with the vendor, including cybersecurity risks, data privacy risks, and operational risks.
- **Approval Process:** Vendors must be approved by the appropriate department heads and must sign a contract that includes terms and conditions related to compliance, confidentiality, and security.

4. Compliance Requirements

- **Legal and Regulatory Compliance:** Vendors must comply with all applicable laws and regulations, including data protection laws, labor laws, environmental regulations, and any industry-specific regulations relevant to the services or products they provide.
- **Security and Data Protection:** Vendors who have access to ZKTeco WFM's sensitive data or systems must adhere to the company's security policies and practices. This includes implementing robust cybersecurity measures, conducting regular security audits, and ensuring data encryption and secure data transfer protocols.
- **Code of Conduct:** Vendors are expected to adhere to ZKTeco WFM's Code of Conduct, which includes ethical business practices, anti-corruption measures, and respect for human rights.

5. Vendor Performance Management

- **Performance Monitoring:** ZKTeco WFM will regularly monitor vendor performance against agreed-upon service levels, key performance indicators (KPIs), and contractual obligations. Performance reviews will be conducted periodically, and any issues or deficiencies will be addressed promptly.

- **Reporting:** Vendors must provide regular reports on their performance, security incidents, compliance with contract terms, and any other relevant metrics. ZKTeco WFM reserves the right to audit vendors to ensure compliance.
- **Continuous Improvement:** ZKTeco WFM encourages vendors to continuously improve their processes and performance. Vendors must be open to feedback and willing to implement corrective actions when necessary.

6. Termination of Vendor Relationships

- **Termination for Non-Compliance:** ZKTeco WFM reserves the right to terminate the relationship with any vendor who fails to comply with the terms of their contract, including non-compliance with legal, regulatory, and security requirements.
- **Exit Strategy:** In the event of termination, ZKTeco WFM will implement an exit strategy to ensure a smooth transition and minimize disruption to operations. This includes the secure transfer of any data, return of company property, and settlement of outstanding obligations.

7. Record Keeping and Documentation

- **Documentation:** All vendor contracts, due diligence records, performance reviews, and compliance reports must be documented and stored securely. These records must be accessible for audit and review purposes.
- **Retention Period:** Vendor-related documentation must be retained for a minimum of five years after the termination of the vendor relationship or as required by applicable law.

8. Roles and Responsibilities

- **Vendor Management Team:** The Vendor Management Team is responsible for overseeing vendor relationships, conducting due diligence, and ensuring compliance with this policy.
- **Department Heads:** Department heads are responsible for approving vendors and ensuring that vendor performance meets the required standards.
- **Compliance Officer:** The Compliance Officer is responsible for ensuring that all vendors adhere to legal and regulatory requirements and for conducting audits as needed.

9. Review and Revision

This policy will be reviewed annually and revised as necessary to reflect changes in legal, regulatory, or business requirements. Any changes to this policy will be communicated to all relevant stakeholders.

10. Policy Acknowledgment

All employees involved in vendor management activities must acknowledge their understanding and acceptance of this policy. Vendors must also acknowledge their understanding of and compliance with the terms outlined in this policy.

ZKTeco WFM Network Security and Monitoring Policy

1. Introduction

This Network Security and Monitoring Policy establishes the framework for securing the corporate network and the CirrusDCS product, hosted on Amazon Web Services (AWS). The policy outlines the necessary measures to protect the network infrastructure, detect potential threats, and ensure continuous monitoring of network activities. This policy aligns with industry best practices and AWS security recommendations.

2. Scope

This policy applies to all corporate network infrastructure components, including those associated with the CirrusDCS product hosted on AWS. It covers network design, access controls, monitoring, threat detection, and incident response.

3. Network Security Principles

1. **Defense in Depth**: Implement multiple layers of security controls across the network to protect against various types of threats.
2. **Zero Trust Architecture**: Assume no implicit trust; all devices, users, and network traffic must be authenticated and authorized.
3. **Segmentation**: Network segments are created to isolate different parts of the network, ensuring that a breach in one area does not compromise the entire infrastructure.
4. **Encryption**: All data transmitted across the network is encrypted, ensuring confidentiality and integrity.

4. Network Design and Configuration

1. **Network Segmentation**:
    - **Virtual Private Cloud (VPC)**: CirrusDCS utilizes AWS VPCs to segment the network. Subnets are created for different components (e.g., application servers, databases, and web servers), and strict access controls are enforced between them.
    - **Security Groups**: Security groups are used to control inbound and outbound traffic to AWS resources, ensuring that only necessary communication is allowed.
2. **Firewalls and Intrusion Prevention**:
    - **AWS Network Firewall**: A network firewall is deployed to inspect and filter traffic at the perimeter of the AWS network. It enforces rules that block unauthorized access and mitigate known threats.
    - **Intrusion Prevention System (IPS)**: An IPS is integrated to detect and prevent known exploits and attacks in real-time. The system is regularly updated with the latest threat intelligence.

- **AWS Web Application Firewall (WAF)**: AWS WAF is used to protect web applications hosted on AWS from common web exploits, such as SQL injection, cross-site scripting (XSS), and DDoS attacks. AWS WAF rules are configured to block malicious traffic while allowing legitimate users to access the services. WAF policies are regularly reviewed and updated based on emerging threats.

3. **Virtual Private Network (VPN)**:
    - **Site-to-Site VPN**: A secure VPN tunnel is established between the corporate network and AWS to ensure secure communication for administrators and authorized users.
    - **Remote Access VPN**: Remote employees and contractors access the corporate network through a secure VPN with multi-factor authentication (MFA).
4. **Domain Name System (DNS) Security**:
    - **Amazon Route 53**: DNS traffic is managed and secured using AWS Route 53. DNS queries are monitored for malicious activity, and Domain Name System Security Extensions (DNSSEC) are used to prevent DNS spoofing.
    - **DNS Filtering**: Malicious domains are blocked at the DNS level, preventing access to known phishing and malware sites.

5. Access Control

1. **Network Access Control Lists (NACLs)**:
    - NACLs are implemented at the subnet level within the VPC to provide an additional layer of security, controlling inbound and outbound traffic to specific subnets.
    - **Least Privilege**: Network access is restricted to the minimum necessary to perform job functions, and access is regularly reviewed.
2. **AWS Identity and Access Management (IAM)**:
    - IAM policies control access to network management resources, ensuring that only authorized personnel can make changes to network configurations.

6. Monitoring and Logging

1. **Network Traffic Monitoring**:
    - **Amazon VPC Flow Logs**: VPC Flow Logs are enabled to capture detailed information about the traffic flowing in and out of the network. These logs are stored securely in AWS CloudWatch Logs or Amazon S3 for analysis.
    - **Amazon GuardDuty**: AWS GuardDuty is enabled to monitor for unusual network activity and potential threats. It provides continuous security monitoring using machine learning, anomaly detection, and integrated threat intelligence.

2. **Logging and Auditing**:
    - **AWS CloudTrail**: CloudTrail is used to log all API calls and actions taken on the AWS network, providing a comprehensive audit trail.
    - **Amazon CloudWatch**: CloudWatch monitors network performance and logs metrics such as latency, error rates, and traffic volume. Alerts are set up for any anomalies or suspicious activities.
3. **Threat Detection and Incident Response**:
    - **Amazon Macie**: Macie is used to monitor and protect sensitive data within the network by identifying and alerting on potential data leaks.
    - **AWS Security Hub**: Security Hub is used to aggregate and prioritize security findings across AWS accounts and services, providing a centralized view of network security posture.
    - **AWS WAF Monitoring**: AWS WAF logs and metrics are monitored through CloudWatch to detect and respond to web application threats. Any anomalous traffic patterns or repeated attack attempts are escalated for immediate investigation and mitigation.

7. Network Security Best Practices

1. **Patch Management**:
    - All network devices and AWS resources are regularly updated with the latest security patches. Automated patch management tools are used to ensure timely application of patches.
2. **Network Hardening**:
    - Unnecessary services and ports are disabled on all network devices and AWS resources. Default passwords are changed, and only strong, complex passwords are used.
3. **Encryption**:
    - **Data in Transit**: All data transmitted over the network is encrypted using TLS 1.2 or higher. This includes data between AWS resources, internal applications, and external services.
    - **Data at Rest**: Data at rest is encrypted using AWS Key Management Service (KMS), ensuring that sensitive information is protected from unauthorized access.
4. **Regular Security Assessments**:
    - Periodic vulnerability scans and penetration tests are conducted to identify and mitigate potential weaknesses in the network. Results are reviewed, and remediation efforts are tracked.

8. Incident Response

1. **Incident Detection**:
    - All network events that indicate potential security incidents are promptly investigated. This includes alerts from intrusion detection systems, anomalous traffic patterns, and unauthorized access attempts.
2. **Incident Containment**:
    - Immediate actions are taken to contain any security breaches, such as isolating affected network segments, blocking malicious IP addresses, and disabling compromised accounts.
3. **Incident Resolution**:
    - The root cause of the incident is identified, and corrective actions are taken to prevent recurrence. Detailed incident reports are prepared and reviewed by the security team.
4. **Communication**:
    - Security incidents are communicated to relevant stakeholders, including senior management, affected users, and customers, as appropriate.

9. Compliance and Review

1. **Compliance Monitoring**:
    - Regular audits are conducted to ensure compliance with this policy and relevant regulatory requirements (e.g., SSAE18 SOC, GDPR). Any non-compliance is addressed with corrective actions.
2. **Policy Review**:
    - This Network Security and Monitoring Policy is reviewed annually or whenever significant changes occur in the network environment, AWS services, or industry standards. Updates to the policy are communicated to all relevant personnel.

ZKTeco WFM Patch Management Policy

Purpose

The purpose of this Patch Management Policy is to ensure the security, availability, and integrity of ZKTeco WFM's cloud-based infrastructure hosted on Amazon Web Services (AWS). Regular patching of systems and applications is crucial to mitigate vulnerabilities that could be exploited by threat actors, thereby protecting company and customer data from unauthorized access or loss.

Scope

This policy applies to all systems, applications, and cloud resources managed by ZKTeco WFM on the AWS platform. It is relevant to all personnel responsible for system and application administration, including third-party service providers.

Policy Overview

ZKTeco WFM is committed to maintaining a secure environment by ensuring that all systems and applications are patched in a timely manner. The following procedures outline the responsibilities and processes necessary to comply with this policy.

Patch Management Procedures

1. **Monitoring and Notification**
    - **Frequency:** System administrators must check for new patches and updates at least weekly by monitoring AWS notifications, relevant vendor sites, and security advisories.
    - **Notifications:** Automated alerts should be configured to notify administrators immediately when critical patches or updates are released.
2. **Patch Testing**
    - **Testing Environment:** All patches must be tested in a dedicated staging environment that replicates the production setup as closely as possible.
    - **Evaluation:** Testing should focus on evaluating the patch's impact on functionality, performance, and security. Compatibility issues must be identified and resolved before deployment.
    - **Documentation:** Test results, including any issues encountered and resolutions, must be documented.
3. **Approval and Change Management**
    - **Approval Process:** Prior to deploying patches to production, they must be reviewed and approved by the Change Management team.
    - **Change Request:** A Change Request (CR) must be submitted detailing the patch, its potential impact, and the results of the testing phase. The CR must be approved by the relevant stakeholders, including IT security and operations teams.

- **Communication:** A communication plan must be established and shared with all relevant teams at least 48 hours before the scheduled deployment. The plan should outline the timing, expected impact, and any required downtime.

4. **Patch Deployment**
    - **Timeline for Critical Patches:** Critical patches must be deployed within 7 days of release to address vulnerabilities that pose significant security risks.
    - **Timeline for Non-Critical Patches:** Non-critical patches should be deployed within 30 days of release.
    - **Rollback Plan:** A rollback plan must be prepared and documented before deployment. This plan should include steps to revert to the previous state in case the patch causes unforeseen issues in the production environment.
    - **Post-Deployment Monitoring:** After deployment, the system should be monitored for stability and functionality. Any anomalies should be addressed immediately, with the rollback plan activated if necessary.
5. **Exception Handling**
    - **Exception Requests:** If a patch cannot be applied within the specified timeline, an exception request must be submitted to and approved by the ZKTeco WFM Management Team. The request must detail the reason for the delay, the risks involved, and any compensating controls in place.
    - **Monthly Review:** Approved exceptions must be reviewed monthly to assess whether the patch can be applied or if further mitigation is required.
6. **Documentation and Compliance**
    - **Record Keeping:** All patching activities, including testing, approvals, deployments, and exceptions, must be documented and stored securely.
    - **Policy Review:** The Patch Management Policy and procedures will be reviewed annually or following significant changes to the infrastructure or security landscape to ensure ongoing relevance and effectiveness.

Roles and Responsibilities

- **System Administrators:** Responsible for monitoring patch releases, testing patches, and coordinating with the Change Management team for deployment.
- **Change Management Team:** Reviews and approves patch deployment plans, ensuring minimal disruption to business operations.
- **Security Team:** Assesses the security implications of patches and provides guidance on priority and urgency.
- **Management Team:** Reviews and approves exception requests, ensuring that risks are appropriately managed.

Review and Maintenance

- The Patch Management Policy will be reviewed annually to ensure it remains current with industry best practices and the evolving threat landscape.
- Any updates or changes to this policy will be documented in the revision history section below.

Document History and Revision Table

Ver.	Date	Description of Changes	Rev. By	App. By	App. Date
1	9/1/2024	Initial creation of the Vendor Management and Compliance Policy	John Doe	Jane Smith	9/2/2024

ZKTeco WFM Service Level Agreement

This Service Level Agreement, (the "SLA"), is a schedule to the Master Services Agreement between ZKTeco and Customer for Hosted Services. Product support is provided by the ZKTeco Customer Support Team. ZKTeco representative is available to support customers as established in the SLA. Support encompasses technical troubleshooting, functional expertise and instruction on the configuration and use of ZKTeco products, as well as general customer service. Capitalized terms have the meanings given to them herein or in the MSA. The term "Month" means calendar month. The terms of the SLA are as follows.

1. Definitions

1.1. **"Customer"** refers to the organization that has signed the Agreement under which it has purchased ZKTeco CirrusDCS Services from ZKTeco.

1.2. **"Downtime"** is defined as any period when Users are unable to access CirrusDCS sites for which they have appropriate permissions. The ability to access the CirrusDCS sites is determined by automated monitoring that attempts to access CirrusDCS sites every minute supplemented by server logs. Downtime does not include the period of time when the Service is not available as a result of (i) Scheduled Downtime or scheduled network, hardware, or service maintenance or upgrades; or (ii) the acts or omissions of Customer or Customer's employees, agents, contractors, or vendors, or anyone gaining access to ZKTeco's network by means of Customer's passwords or equipment; or (iii) Customer requested changes.

1.3. **"Downtime Service Credits"** is the percentage of the monthly service fees for the Service that is credited to Customer for a Service Level not met under this SLA.

Monthly Uptime Percentage	Service Credit
< 99%	20%
< 96%	40%
< 94%	60%
< 92%	80%
< 90%	100%

1.4. **"Monthly Uptime Percentage"** for a specific customer is calculated as follows:

$$100 - (\mathbf{x}/\mathbf{y} \times 100)$$

Where x = number of downtime hours; y = number of hours in the calendar month.

For example, if x = 2 hours in the month of April (y = 760 hours), the calculation outcome is ~99.74%.

1.5. **"Service Level"** means standards ZKTeco adheres to and by which it measures the level of service it provides as expressly set forth below.

1.6. **"Scheduled Downtime"** is defined as (i) Downtime within pre-established maintenance windows; customer-specific updates or customization; general upgrades to firmware or (ii) Downtime during major version upgrade; Scheduled Downtime is not considered Downtime for purposes of this SLA.

2. Exclusions

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

(a) Due to factors outside ZKTeco's reasonable control;
(b) That resulted from Customer's or third-party hardware or software;
(c) That resulted from actions or inactions of Customer or third parties;
(d) Issues caused by Customer's use of the Service after ZKTeco advised Customer to modify its use of the Service. If Customer did not change its use as advised, ZKTeco is not responsible
(e) During scheduled downtime; or
(f) During beta and trial services (as determined by ZKTeco).

3. Downtime Service Credit

(a) The amount and method of calculation of Downtime Service Credits are described below in connection with each Service Level description.
(b) Downtime Service Credits are Customer's sole and exclusive financial remedy for any violation of this SLA.
(c) The Downtime Service Credits awarded in any calendar month shall not, under any circumstance, exceed credits equal to one Month, and
(d) The value of the Downtime Service Credits awarded (calculated by totaling the monetary value of the monthly service fees credited to Customer) may not exceed 20% of Customer's Hosted Service fees paid during the twelve (12) consecutive Months between anniversaries of the Effective Date.
(e) For Services purchased as part of a suite, the Downtime Service Credits will be based on the pro-rata portion of the estimated retail price of the Service, as determined by ZKTeco in its reasonable discretion.
(f) Downtime Service Credits do not apply to one-time fees associated with this service.
(g) ZKTeco provides this SLA subject to the following terms.

4. These terms will be fixed for the duration of the initial Term of the subscription. When customer subscription is renewed, the version of the SLA that is current at the time the renewal term commences will apply throughout the renewal Term.

5. Service Level and Response Time. Customer support requests are classified into multiple service levels, which differ in response time depending upon the effect the failure has on overall system performance, data throughput, or time clock usability.

6. Service Levels. The ZKTeco support team provides the following service levels:
Priority P0: (Critical)

Overview: A critical severity issue causing a Customer's employee data collection operation to stop. The clocks become unusable or are otherwise inaccessible in the Customer's environment.

Qualifying conditions:
- Time clocks: all clocks are down, and employees are not able to punch
- Time clocks: all employee punches are incorrect or missing
- ZK DCS: the service is down due to the failure of the hosting system, web server, database server or the application.

Service Level:
- ZK technical support or engineering responds to the call within a one-hour time frame and goes online to work with the customer on root-cause analysis.
- The customer receives a direct communication every 4 hours with a status update. Please note that ZKTeco will provide updates in 4-hour intervals around the clock via ZKTeco's US-based and offshore support centers.

Priority P1: (High)

Overview: A high severity issue has a significant impact on the Customer's employee data collection process. The Customer's system functions but at a significantly reduced capacity.

Qualifying conditions:

- Time clock: the clock is operational, but employee punch data cannot be sent to the CIRRUS DCS service
- Time clock: the clock is functional and accepts employee punches but disconnects from the network.
- Time clock: the admin user cannot access admin menu due to a permission setup or password issue.
- CIRRUS DCS: The Service fails to load new employee data from the HCM/Workforce Management Hosted Software
    - CIRRUS DCS: The Service fails to submit time clock data to the HCM/Workforce Management Hosted Software
    - CIRRUS DCS: intended employee data is not available on the clock

Service Level:

- ZK responds to the call within a 4-hour time frame during business hours and goes online to work with the Customer on root-cause analysis.
- The Customer receives a direct communication twice a day with a status update.

Priority P2: (Medium)

Overview: A medium severity issue results in some functionality loss on the Customer's employee data collection system. The system remains usable but does not provide an expected functionality most conveniently or expeditiously.

Qualifying conditions:

- Non-critical issues reported by the Customer or time clock users that might not affect the employee punch process, but do affect time clock usability from an end user perspective.

Service Level:

- ZKTeco responds to the call within an 8-hour time frame and provides online or email response regarding progress on the root-cause analysis.
- The Customer receives a direct communication once a day with a status update.

Priority P3: (Low)

Overview:

- Low severity issues include general usage questions, issues related to using of the time clocks or feature requests. There is no impact on the quality, performance or functionality on the Customer's employee data collection system.

Qualifying conditions:

- Time clock functionality changes, CIRRUS DCS feature improvements, or future systems-level change requests from the Customer.
- Can be used to support such as demo sites or evaluative clock testing

Service Level:

- ZKTeco responds to the call within two days and provides an email response to the Customer.

- The Customer receives an update once a week with a status update.

Customer must request all support through a dedicated CirrusDCS support portal at the following link. Customer must ask account access for the support portal in advance from the CirrusDCS support team. Support Portal URL: http://support.zktechnology.com/servicedesk/customer/portals

7. Effective Period

7.1. This Agreement is deemed valid from the Effective Date throughout the subscription period of CIRRUS DCS subscribed by the Customer with the subscription fees confirmed paid to ZKTeco.

8. Changes to SLA

8.1. ZKTeco reserves the right to revised this SLA from time to time to improve ZKTeco's support quality. Any such change or revision to this SLA shall not result in a reduction in service quality. The updated SLA will be published by ZKTeco, and the customers will be notified by email.

ZKTeco WFM CirrusDCS Services Privacy Policy

Last Modified: January 2024

This Privacy Policy (the “Policy”) covers the privacy practices ZKTeco employs when ZKTeco customers (“Customers”) use our cloud-based enterprise applications, including biometric data privacy practices, when applicable (the “Services”). This Privacy Policy does not cover any information or data collected by ZKTeco for other purposes, such as information collected on the ZKTeco website or for marketing purposes. Capitalized terms used but not defined in this Policy shall have the meaning given to them in the Master Services Agreement (the “Agreement”).

1. **Collection and Use of Personal Data**

1.1. **Personal Data ZKTeco Processes**. In the normal course of using the Services, Customer employees will input electronic data (“Customer Data”) and biometric data (“Biometric Data”) into the ZKTeco systems (“Customer Personal Data”). The use of information collected through the Services shall be limited to the data necessary to provide Services for which the Customer has engaged ZKTeco, as described in the Agreement. ZKTeco may access Customer Data for the purposes of providing the Services, preventing or addressing service or technical problems, responding to support issues, and responding to Customer’s instructions, or as may be required by law, in accordance with the relevant Agreement between Customer and ZKTeco.

1.2. **Data Processing**. ZKTeco processes Customer Personal Data under the direction of Customer, and has no direct control or ownership of the Customer Personal Data it processes. Customers are responsible for complying with any regulations or laws that require providing notice, disclosure, and/or obtaining consent prior to transferring the data to ZKTeco for processing purposes. Customer Personal Data processed from outside the United States (“US”) is handled as described in section 2 of this Policy and the ZKTeco Data Processing Agreement.

1.3. **Editing or Deleting Personal Data**. Any person who seeks access, or who seeks to correct, amend, or delete inaccurate data, should direct their query to the ZKTeco Customer (the data controller). If the Customer instructs ZKTeco to remove the personal data to comply with data protection regulations, ZKTeco will respond to their request within 30 days.

1.4. **Disclosure to Law Enforcement**. ZKTeco will refer any request for disclosure of personal data by a law enforcement authority to the Customer. ZKTeco may, where it concludes that it is legally obligated to do so, disclose personal data to law enforcement or other government authorities. ZKTeco will notify Customer of such request unless prohibited by law.

1.5. **Accessing the Services**. Customers and their authorized users may access the Services directly through a URL unique to their individual tenant, or may elect to use internal launch pages for single sign-on or other purposes. Customers input information for processing and storage as they use the Services. Customers may also configure the Services to allow end users to input information directly into the Services.

2. Global Data Privacy. Providing Services to Customers with employees outside of the US may require the transfer of Customer Personal Data to the US (e.g., when Customer hosts its HCM/Workforce Management Hosted Software tenant in the United States).

3. **US-EU Data Privacy Framework**. ZKTeco may transfer Customer Personal Data internationally, at the direction of Customer, to provide Services as established in the Agreement. ZKTeco has taken appropriate safeguards to require that Customer Personal Data will remain protected. For transfers of PI originating in the EU to the US for processing, ZKTeco will comply with the U.S.-EU and U.S.-Swiss Privacy Framework. See the Data Privacy Framework Policy for more details on the Data Privacy.

4. **Biometric Information.** The biometric data covered by this policy includes “Biometric Identifiers” as defined by the Illinois Biometric Information Privacy Act (“BIPA”) (i.e., a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and “Biometric Information” as defined by BIPA (i.e., any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s Biometric Identifier used to identify an individual), together “Biometric Data”. At the direction and on behalf of its Customers, ZKTeco may collect, store and/or use Biometric Data. Customers may utilize ZKTeco’s products and services to collect, store and/or use Biometric Data solely for employment-related purposes, including tracking of time and attendance, in accordance with this policy and applicable law.

4.1. Customer’s Responsibilities. It is the sole responsibility of the Customer that collects, captures, stores, or otherwise uses Biometric Data relating to an individual, to:

4.1.1. Inform the individual from whom Biometric Data will be collected, in writing and prior to collecting the individual’s Biometric Data, that Biometric Data is being collected, stored, and/or used.

4.1.2. Indicate, in writing, the specific purpose(s) and length of time for which Biometric Data is being collected, stored, and/or used.

4.1.3. Receive a written release from the individual (or a legally authorized representative) authorizing the Customer and ZKTeco to collect, store, and/or use the Biometric Data and authorizing the Customer to disclose such Biometric Data to ZKTeco and any Customer third-party service providers.

4.1.4. Develop, maintain, and to inform all individuals about any Customer policies for Biometric Data collection. Customer must maintain its own data collection, disclosure, retention, and storage policies in compliance with all applicable laws. Where required by law, Customer agrees to adopt a privacy policy in alignment all applicable laws governing the collection, use, transfer and retention of Personal Data.

4.1.5. Ensure that ZKTeco is immediately notified upon termination or other discontinuation of use of ZKTeco’s biometric products or services with respect to an employee or other individual.

4.2. Disclosure and Sharing of Biometric Information

4.2.1. ZKTeco will not sell, lease, trade or otherwise profit from any biometric data that it receives from Customer’s employees. Biometric data will not be used for any purpose other than as described herein.

4.2.2. ZKTeco will not disclose, redisclose or otherwise disseminate any biometric data received from Customers to any person or entity other than ZKTeco and ZKTeco’s third party service providers except for if disclosure or redisclosure is required by state or federal law or municipal ordinance or disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

4.3. Illinois Biometric Information Privacy Act. In accordance with the Illinois Biometric Information Privacy Act (740 Ill. Comp. Stat. Ann. 14/1 et seq.) (the “Illinois BIPA”), ZKTeco maintains comprehensive policies and procedures to ensure the proper collection, use, safeguarding, storage, retention, and destruction of Biometric Data by ZKTeco. As required by the Illinois BIPA, ZKTeco makes available to the public its Biometric Data Retention and Storage policies in the following sections.

4.4. **Retention of Biometric Information**. ZKTeco will retain biometric data until the initial purpose for collecting or obtaining such biometric data has been satisfied, or within three (3) years of an individual’s last interaction with the Client and/or ZKTeco, as applicable, whichever occurs first, at

which time ZKTeco will permanently delete such biometric data and shall demand that its vendors do the same. When instructed by its customers to destroy biometric data, ZKTeco will promptly comply with the request. ZKTeco will destroy all biometric data from former or inactive customers who fail to destroy such data.

4.5. **Storage of Biometric Information**. ZKTeco will use a reasonable standard of care, consistent with the industry in which ZKTeco operates, to store, transmit and protect from disclosure all biometric data, and shall store, transmit, and protect from disclosure all biometric data in a manner that is the same as or more protective than the manner in which ZKTeco stores, transmits, and protects other confidential or sensitive data that can be used to uniquely identify an individual or an individual's account or property.

5. Additional ZKTeco Privacy Information

5.1. **Data Retention**. ZKTeco retains Customer Personal Data for as long as necessary to fulfill the purposes for which it is processed. ZKTeco standard retention period for Customer Personal Data is ninety seven (97) days unless Customer opts to retain Customer Personal Data for a longer period of time for business purposes. ZKTeco's retention practices comply with applicable data protection laws. When the retention period has expired, Customer Personal Data will be securely deleted or destroyed.

5.2. **Security**. The security of Customer Personal Data, including personal data, is very important to ZKTeco. ZKTeco maintains a comprehensive, written information security program that contains industry-standard, administrative, technical, and physical safeguards designed to prevent unauthorized access to Customer Personal Data. ZKTeco designs its applications to allow Customers to achieve differentiated configurations, enforce user access controls, and manage data categories that may be populated and/or made accessible on a geographical basis. Configuring these settings appropriately is the Customer's responsibility. Customer may hire ZKTeco to implement the application and/or to make adjustments through ongoing support, but Customer is responsible for establishing user access controls and policies. Additional information about the security settings and configurations can be found in the ZKTeco Documentation made available to Customers.

5.3. **Changes to this Privacy Policy**. We reserve the right to change or update this Privacy Policy at any time. Changes to the Privacy Policy will be posted on this website and links to the Privacy Policy will indicate that the policy has been changed or updated. We encourage you to periodically review this Privacy Policy for any changes. For new Customers, changes or updates are effective upon posting. For existing Customers, changes or updates are effective 30 days after posting.

5.4. **Compliance**. ZKTeco has appointed a chief security officer responsible for overseeing the implementation of the privacy program within the organization. If you have further questions related to this policy, please ask your Customer Support contact to log a customer care case with the privacy question.

6. Contact Information

6.1. If you have any questions regarding our Privacy Statement, or if at any time after providing your personal information to ZKTeco you want to update, change, unsubscribe, or request removal or deletion of your information, or if you would like to assert any of the rights listed above, please direct your request via the postal mail address listed below. ZKTeco will respond to your request within a reasonable timeframe.

6.2. **ZKTeco Contact Address**:

ZKTeco
Attn: Chief Security Officer
200 Centennial Avenue, Suite 211
Piscataway, NJ 08854

ZKTeco WFM Data Privacy Framework Policy

Last Modified: January 2024

This Data Privacy Framework Policy ("Policy") (*formerly Privacy Shield*) describes how ZKTeco ("ZKTeco," "we," "us" or "our") collects, uses, and discloses certain personally identifiable information that we receive in the United States from the European Union ("EU Personal Data"), the United Kingdom ("UK Personal Data"), and Switzerland ("Swiss Personal Data" and combined with EU Personal Data and UK Personal Data, the "Personal Data"). This Policy applies to all of our United States legal entities, subsidiaries and/or affiliates that exist now or in the future. This Policy supplements our Website Privacy Policy and Terms of Use located at [INSERT LINK].

1. **Commitment to Compliance**.

    a. ZKTeco complies with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the U.S. Department of Commerce. ZKTeco has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (the "EU-U.S. DPF Principles") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. ZKTeco has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (the "Swiss-U.S. DPF Principles") with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

    b. ZKTeco commits to cooperate and comply respectively with the advice of the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship.

    c. If there is any conflict between the terms in this Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles (collectively, the "Principals"), the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program (the "DPF Program"), please visit https://www.dataprivacyframework.gov/.

    d. ZKTeco recognizes that the EU, UK, and Switzerland have established strict protections regarding the handling of Personal Data, including requirements to provide adequate protection for Personal Data transferred outside of their respective jurisdictions. To provide adequate protection for all Personal Data regarding consumers, clients, suppliers, business partners, job applicants and employees received in the US, ZKTeco has elected to self-certify to the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF administered by the US Department of Commerce. ZKTeco adheres to the EU-US Data Privacy Framework Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability.

    e. The Federal Trade Commission has jurisdiction over ZKTeco's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

    f. To review ZKTeco's representation on the Data Privacy Framework List, see the U.S. Department of Commerce's Data Privacy Framework List located at https://www.dataprivacyframework.gov/s/participant-search.

2. **Personal Data Collection and Use.** We may receive the following categories of Personal Data in the U.S.: (i) employment and HR information; (ii) commercial information; (iii) demographic information; and (iv) consumer-specific information (including biometric information).

a. Within these categories, we may collect information such as an individual's name, location, name of employer, professional role, job qualifications (such as educational degrees earned), phone number, email address, user ID, biometric template, and badge ID.

b. We process Personal Data for the following purposes: (i) to provide our services, including with respect to billing, identification, and authentication; (ii) to contact and communicate with our clients regarding our services, and (iii) for employment-related purposes including to process employment-related data in the U.S. and evaluate job candidates. Data subjects whose personally identifiable information we process include clients (and their respective employees or other users) and other legal persons, suppliers, business partners, job applicants, independent contractors, and employees.

c. We will only process Personal Data in ways that are compatible with the purpose of collection, or for purposes, the individual later authorizes. Before we use your Personal Data for a purpose that is materially different than the purpose we collected it for, or that you later authorized, we will provide you with the opportunity to opt out. We maintain reasonable procedures to help ensure that Personal Data is reliable for its intended use, accurate, complete, and current.

d. We may collect the following categories of sensitive Personal Data including but not limited to:, criminal history, and biometric template information as may be required by our customers, for identification of their employees, within the employment context. When we collect sensitive Personal Data, we will obtain your opt-in consent where the EU-U.S. DPF requires, including if we disclose your sensitive Personal Data to third parties, or before we use your sensitive Personal Data for a different purpose than we collected it for or than you later authorized. Certain exceptions to our obligation to obtain affirmative opt-in consent to process sensitive personal data are where the processing is: (i) in the vital interests of the individual or another person; (ii) necessary for the establishment of legal claims or defenses; (iii) required to provide medical care or diagnosis; (iv) carried out in the course of legitimate activities by certain foundations, associations, or other non-profit bodies; (v) necessary to carry out employment law-related obligations; (vi) related to data made public by the individual.

e. ZKTECO commits to cooperate with the EU/EEA data protection authorities, the UK Information Commissioner's Office and the Gibraltar Regulatory Authority, and the Swiss Data Protection and Information Commissioner and comply with the requirements of such authorities with regard to Personal Data transferred from the EU, the UK, and Switzerland.

3. **Data Transfers to Third Parties.** We may transfer Personal Data to our third-party agents or service providers who perform functions on our behalf. ZKTECO will select third party agents or service providers who comply with the DPF Program, and are limiting their use of the data to the specified services provided on our behalf, in order to provide the same level of protection that the DPF Program requires, We take reasonable and appropriate steps to ensure that third-party agents and service providers process Personal Data in accordance with our DPF Program obligations and to stop and remediate any unauthorized processing. Under certain circumstances, we may remain liable for the acts of our third-party agents or service providers who perform services on our behalf for their handling of Personal Data that we transfer to them.

4. **Disclosures for National Security or Law Enforcement.** Under certain circumstances, we may be required to disclose your Personal Data in response to valid requests by public authorities, including to meet national security or law enforcement requirements, or as otherwise required by law. ZKTECO is not liable for the use or re-disclosure of Personal Data by such recipients.

5. **Security**. We maintain reasonable and appropriate security measures to protect Personal Data from loss, misuse, unauthorized access, disclosure, alteration, or destruction in accordance with the DPF Program.

6. **Access Rights**. You may have the right to access the Personal Data that we hold about you and to request that we correct, amend, or delete it if it is inaccurate or processed in violation of the DPF Program. These access rights may not apply in some cases, including where providing access is unreasonably burdensome or expensive under the circumstances, or where it would violate the rights of someone other than the individual requesting access or where the data is controlled by your employer who acts as the Data Controller. If you would like to request access to, correction, amendment, or deletion of your Personal Data, you can contact ZKTeco at: privacy@ZKTechnology.com.

7. **Questions or Complaints.**

    a. In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, ZKTeco commits to resolve complaints about our collection or use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints regarding our Policy should first contact ZKTECO at: privacy@ZKTechnology.com.

    b. In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, ZKTECO commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://www.jamsadr.com/DPF-Dispute-Resolution for more information or to file a complaint. The services of JAMS are provided at no cost to you.

    c. We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of your Personal Data within 45 days of receiving your complaint.

8. **Binding Arbitration.** You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: (1) raised your complaint directly with us and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified above; and (3) raised the issue through the relevant data protection authority and allowed the U.S. Department of Commerce an opportunity to resolve the complaint at no cost to you. For more information on binding arbitration, see U.S. Department of Commerce's EU-U.S. DPF: Annex I of the DPF Principles.

9. **Contact Us**. If you have any questions about this Policy or would like to request access to your Personal Data, please contact us at privacy@ZKTechnology.com.

10. **Changes to This Policy**. We reserve the right to amend this Policy from time to time to be consistent with the DPF Program's requirements.

ZKTeco WFM Access Control Policy

1. Introduction

This Access Control Policy outlines the procedures and standards for managing access to corporate resources and the CirrusDCS product, which is hosted on Amazon Web Services (AWS). The goal is to ensure that access is granted only to authorized individuals and that all actions are traceable to specific users. This policy is designed to align with industry best practices and AWS security recommendations.

2. Scope

This policy applies to all employees, contractors, partners, and third-party vendors who require access to corporate systems and the CirrusDCS product hosted on AWS. It covers all physical and logical access to systems, data, and network resources.

3. Access Control Principles

1. **Least Privilege**: Access to resources is granted based on the principle of least privilege. Users are given the minimum level of access required to perform their job functions.
2. **Role-Based Access Control (RBAC)**: Access rights are assigned based on user roles within the organization. Roles are defined according to job responsibilities, and access permissions are tailored to each role.
3. **Need-to-Know Basis**: Access to sensitive data and systems is granted only to individuals who require it to fulfill their job duties.
4. **Separation of Duties**: Where possible, tasks are divided among multiple individuals to reduce the risk of unauthorized access or fraud.

4. Access Management

1. **User Account Management**:
    a. **Provisioning**: User accounts are created upon approval by the department head or authorized manager. Access is granted based on predefined roles.
    b. **De-provisioning**: User accounts are promptly disabled or deleted upon termination of employment or when access is no longer required.
    c. **Regular Review**: Access rights are reviewed periodically (at least quarterly) to ensure that users have appropriate access levels. Any unnecessary access is removed immediately.
2. **Authentication Mechanisms**:
    a. **Multi-Factor Authentication (MFA)**: All users with access to AWS resources and CirrusDCS must use MFA to authenticate. MFA includes the use of passwords combined with a secondary authentication method (e.g., SMS code, authenticator app).
    b. **Password Policy**: Passwords must be complex, at least 12 characters long, and include a mix of upper and lower case letters, numbers, and special characters. Passwords must be changed every 90 days.

3. **AWS Identity and Access Management (IAM)**:

a. **IAM Policies**: Access to AWS resources is controlled using IAM policies, which are attached to users, groups, and roles. Policies are crafted to grant the least privilege necessary.
b. **Roles and Permissions**: IAM roles are used to delegate access to AWS resources, allowing secure access to resources without sharing credentials.
c. **AWS Organizations**: If applicable, AWS Organizations is used to manage multiple AWS accounts, with Service Control Policies (SCPs) applied to enforce governance rules across the organization.

5. Access Control to CirrusDCS

1. **Data Access**:
    a. **Data Segmentation**: Data within CirrusDCS is segmented based on sensitivity and access levels, ensuring that users can only access the data necessary for their role.
    b. **Encryption**: All data, both in transit and at rest, is encrypted using AWS-provided encryption services (e.g., KMS for data at rest, TLS for data in transit).
2. **Logging and Monitoring**:
    a. **AWS CloudTrail**: All access to AWS resources is logged using AWS CloudTrail, providing a full audit trail of user activity.
    b. **Amazon CloudWatch**: CloudWatch is used to monitor and alert on specific access patterns, unusual activity, or failed login attempts.
    c. **AWS Config**: AWS Config is utilized to track changes in AWS resource configurations, ensuring compliance with the access control policy.
3. **Access to the CirrusDCS Application**:
    a. **Application-Level Access**: Access to the CirrusDCS application is controlled through role-based permissions within the application itself. Only authenticated users can access the system, and their actions are logged.
    b. **API Access**: Access to CirrusDCS via API is secured using AWS API Gateway, with strict authentication and authorization checks in place.

6. Third-Party Access

1. **Vendor Management**:
    a. **Contractual Obligations**: Third-party vendors with access to corporate systems or CirrusDCS must agree to adhere to this Access Control Policy.
    b. **Access Review**: Third-party access is reviewed regularly, and permissions are revoked immediately when no longer necessary.
2. **Third-Party Access Control**:
    a. **Least Privilege**: Third parties are granted the minimum access necessary to perform their functions.
    b. **Monitoring**: All third-party access is monitored and logged, with alerts set up for any unusual activity.

7. Incident Response

1. **Access Breach**: In the event of an access breach, immediate action will be taken to revoke access, assess the scope of the breach, and mitigate any potential damage.

2. **Reporting**: All access-related incidents must be reported to the Security Team immediately. A full investigation will be conducted, and appropriate actions will be taken to prevent future incidents.

8. Policy Compliance

1. **Compliance Monitoring**: Regular audits and compliance checks will be performed to ensure adherence to this Access Control Policy.
2. **Non-Compliance**: Any violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

9. Policy Review

This Access Control Policy will be reviewed annually or whenever there are significant changes to the corporate environment, AWS services, or industry best practices. Any changes to the policy will be communicated to all relevant stakeholders.

ZKTeco WFM Employee Security Awareness and Training Policy

1. Introduction

The Employment Awareness and Training Policy is a critical component of the Corporate Security Policy, designed to ensure that all employees, contractors, and relevant third parties understand the security risks associated with their roles and are equipped with the knowledge and skills necessary to protect corporate assets. This policy outlines the framework for security awareness programs and training initiatives across the organization.

2. Scope

This policy applies to all employees, contractors, temporary staff, and third-party vendors who have access to the organization's information systems, networks, or data. It covers mandatory security training, ongoing awareness initiatives, and specialized training for roles with elevated security responsibilities.

3. Policy Objectives

The objectives of this policy are to:

1. Foster a culture of security awareness throughout the organization.
2. Ensure all personnel understand their roles and responsibilities in safeguarding corporate assets.
3. Provide ongoing education on current security threats and best practices.
4. Equip employees with the necessary skills to identify and respond to security incidents.
5. Maintain compliance with relevant legal, regulatory, and contractual security requirements.

4. Roles and Responsibilities

1. **Security Team**:
    - Develops and maintains the security awareness and training program.
    - Conducts regular assessments of the training program’s effectiveness.
    - Updates training materials to reflect the latest security threats and best practices.
2. **Human Resources (HR)**:
    - Ensures all new hires complete mandatory security training as part of the onboarding process.
    - Tracks employee completion of required training courses.

3. **Department Heads/Managers**:

- Ensure that team members complete mandatory training.
- Identify roles that require specialized security training and coordinate with the Security Team to provide it.

4. **Employees**:
    - Participate in all required security training and awareness programs.
    - Apply the knowledge and skills gained from training to their daily work activities.
    - Report any security incidents or suspicious activities in accordance with the Incident Response Policy.

5. Security Awareness Program

1. **Mandatory Security Training**:
    - **Onboarding**: All new hires must complete mandatory security training within the first two weeks of employment. This training includes topics such as password management, phishing awareness, data protection, and secure use of company devices.
    - **Annual Refresher Training**: All employees are required to complete an annual security refresher course to reinforce key security principles and update employees on new threats and security policies.
2. **Ongoing Security Awareness Initiatives**:
    - **Phishing Simulations**: Regular phishing simulation exercises are conducted to test employees' ability to identify and report phishing attempts. Results are used to tailor additional training where needed.
    - **Security Newsletters**: Monthly newsletters are distributed to all employees, highlighting recent security incidents, new threats, and tips for maintaining security.
    - **Security Awareness Week**: An annual event dedicated to promoting security awareness through workshops, guest speakers, and interactive sessions.
3. **Specialized Training**:
    - **Role-Specific Training**: Employees in roles with elevated security responsibilities (e.g., IT administrators, developers, finance) receive additional, specialized training tailored to the security risks associated with their positions.
    - **Third-Party Vendors**: Vendors with access to corporate systems or data are required to undergo security training aligned with their level of access and responsibility.
4. **Training for Remote Workers**:

- Remote employees are provided with additional training on secure remote work practices, including VPN usage, secure communication tools, and home network security.

6. Monitoring and Compliance

1. **Tracking Training Completion**:
    - HR, in collaboration with the Security Team, tracks the completion of all mandatory security training. Employees who fail to complete required training within the specified timeframe may face disciplinary action.
2. **Assessing Program Effectiveness**:
    - The effectiveness of the security awareness and training program is regularly assessed through employee surveys, phishing test results, and security incident trends. Adjustments to the program are made as needed to address identified gaps.
3. **Continuous Improvement**:
    - The Security Team continuously reviews and updates training materials and awareness initiatives to keep pace with evolving security threats and changes in the organization’s technology and processes.

7. Incident Reporting and Response

Employees are encouraged to report any security incidents or suspicious activities immediately. Reports can be made through the designated incident reporting system or directly to the Security Team. Prompt reporting allows for quick response and mitigation of potential threats.

8. Policy Review

This Employment Awareness and Training Policy is reviewed annually or whenever significant changes occur in the security landscape, corporate infrastructure, or legal and regulatory requirements. Any updates to the policy will be communicated to all relevant personnel.

This policy is designed to cultivate a security-conscious workforce, ensuring that all employees are informed, vigilant, and proactive in protecting the organization's assets and data.

ZKTeco WFM Data Disposal and Destruction Policy

Effective Date: [Insert Date]
Version: 1.0
Last Updated: [Insert Date]
Approved By: Jaimin Shah, CEO

1. Purpose

The purpose of this policy is to establish guidelines for the secure disposal and destruction of sensitive data, including Personal Data, Biometric Data, and any other confidential information, stored on various devices and media within ZKTeco WFM, including old laptops, hard drives, removable media, and cloud storage systems. This policy is designed to ensure compliance with applicable Data Protection Laws (such as GDPR, CCPA, and BIPA) and to prevent unauthorized access to or disclosure of sensitive data.

2. Scope

This policy applies to:

- All ZKTeco WFM employees, contractors, vendors, and any other third-party users with access to ZKTeco WFM systems and data.
- All types of data stored on laptops, desktops, servers, cloud storage, removable media (USB drives, CDs, etc.), and other electronic storage devices.
- The disposal and destruction of both physical and electronic data, including hard copies of documents containing Personal Data or sensitive information.

3. Definitions

- **Personal Data**: Any information that relates to an identified or identifiable individual (e.g., name, email address, biometric identifiers).
- **Data Destruction**: The process of rendering data unreadable and unrecoverable from electronic devices or physical media.
- **Data Disposal**: The physical removal of devices, media, or documents containing sensitive data from ZKTeco's facilities after ensuring proper destruction.
- **Media**: Any physical or electronic material on which data can be stored (e.g., laptops, hard drives, USB drives, etc.).
- **Sensitive Data**: Includes Personal Data, Biometric Data, intellectual property, and other confidential information critical to ZKTeco's operations or customers.

4. Policy Statements

4.1 Data Destruction Procedures

ZKTeco WFM will follow the following guidelines for data destruction:

4.1.1 Electronic Data Destruction

- **Hard Drives and Laptops**:
    - Before decommissioning old laptops or hard drives, ZKTeco will use certified data wiping tools that comply with industry standards (e.g., DoD 5220.22-M or NIST SP 800-88) to overwrite all data, rendering it unrecoverable.
    - In cases where wiping is not feasible or effective, physical destruction of hard drives (e.g., shredding or degaussing) will be performed by certified third-party vendors or using in-house approved methods.
- **Removable Media (USB Drives, CDs, DVDs, etc.)**:
    - Data on removable media must be securely erased using software tools or physically destroyed by shredding, breaking, or degaussing before disposal.
- **Cloud Storage**:
    - For data stored in cloud environments, ZKTeco will ensure data deletion is performed according to the cloud provider's standards and applicable contractual agreements.
    - Data deletion requests must be documented, and reports confirming deletion must be obtained.

4.1.2 Physical Document Destruction

- All hard copies of sensitive documents must be shredded using cross-cut shredders before disposal.
- If physical documents are stored by third-party providers, ZKTeco will verify that they adhere to proper document destruction protocols, including certification of destruction.

4.2 Data Disposal Procedures

- **Electronic Devices**:
    - Once data has been securely destroyed, laptops, desktops, servers, and other electronic devices must be disposed of using environmentally responsible and compliant electronic waste disposal methods.
    - Disposal must be done in accordance with applicable environmental laws and regulations (e.g., WEEE Directive).
- **Removable Media and Devices**:
    - Devices such as USB drives, CDs, and other removable media must be physically destroyed or rendered unusable before disposal.
- **Cloud Storage**:
    - Data stored in third-party cloud systems must be securely deleted upon termination of service. Written confirmation of data destruction from the service provider must be obtained and retained for audit purposes.

4.3 Data Retention Periods and Exceptions

- ZKTeco will retain data in accordance with the **Data Retention Policy**. Once the retention period has expired, or the data is no longer required for business or legal purposes, it must be securely destroyed.
- Data that must be retained for legal or regulatory purposes beyond the normal retention period will be securely archived and access limited. Exceptions must be approved by the Chief Security Officer.

5. Roles and Responsibilities

- **Employees and Contractors**:
  Employees and contractors are responsible for following the procedures outlined in this policy and ensuring that no sensitive data is left on old laptops, devices, or media prior to disposal.
- **IT Department**:
  The IT Department is responsible for securely wiping or physically destroying electronic media and for coordinating with approved vendors for certified data destruction services when needed.
- **Compliance Team**:
  The Compliance Team will regularly audit the data destruction process to ensure compliance with applicable data protection regulations.
- **Chief Security Officer**:
  The Chief Security Officer is responsible for overseeing the implementation and enforcement of this policy, including approving exceptions and managing third-party destruction vendors.

6. Verification and Audits

- ZKTeco will maintain records of all data destruction activities, including certificates of destruction from third-party vendors, for a minimum of three years.
- Regular audits of the data disposal and destruction process will be conducted to ensure compliance with this policy and to identify potential areas for improvement.
- The Compliance Team will conduct periodic checks to verify that data destruction procedures are followed, and any deviations will be reported to senior management.

7. Third-Party Vendors

If third-party vendors are used for data destruction, ZKTeco must ensure that:

- The vendor complies with all applicable data protection regulations (e.g., GDPR, CCPA, BIPA).
- The vendor provides certification of data destruction upon completion.
- Vendor contracts include appropriate data protection clauses and assurances that data destruction will be carried out in a secure and compliant manner.

8. Policy Review and Updates

This policy will be reviewed annually or when there are significant changes in technology, regulations, or business operations that impact data destruction practices. Any updates or changes will be communicated to all employees, contractors, and third-party vendors.

9. Violations of the Policy

Failure to comply with this Data Disposal and Destruction Policy may result in disciplinary action, including termination of employment or contracts, and may also expose ZKTeco to legal and financial liabilities.

10. Contact Information

For questions regarding this policy or to report a potential violation, please contact:

ZKTeco
Attn: Chief Security Officer
200 Centennial Avenue, Suite 211
Piscataway, NJ 08854
Email: [security@zktecowfm.com]

Vendor Assessment:

(Collect SOC Audit for below Vendors)

1. **Microsoft**
2. **Atlassian**
3. **AWS**
4. **nCloud**
5. **ZOHO**
6. **Nextiva**

HR:

1. **Hirin**