MARKHRiS
Your Partner in People Management

SECURITY
White Paper

Cloud Payroll & HR System Security Framework

Excel Systems Sdn Bhd 198901005501(182806 W)
7-2 & 7-3, Jalan PJU 8/5F, Bandar Damansara Perdana, PJU 8 Bukit Lanjan, 47820 Petaling Jaya, Selangor.
Tel : 603 - 7727 3892 (4 hunting lines) **Toll Free:** 1700 819 397 **Website:** https://markhris.com/

EXECUTIVE SUMMARY

Business Resilience & Compliance

MARKHRiS Cloud Payroll & HR System, developed by Excel Systems Sdn Bhd, is a secure, cloud-based Human Resource Management platform designed to support payroll processing, employee data management, and HR operational workflows for enterprise organizations. The platform is engineered with a security-first architecture that prioritizes the confidentiality, integrity, and availability of sensitive HR and payroll data.

MARKHRiS operates on a secure private cloud infrastructure hosted in a Tier-3 data center in Malaysia, managed by certified cloud service providers. The platform is further enhanced with Microsoft Azure Arc integration, enabling centralized policy enforcement, security monitoring, and hybrid infrastructure governance.

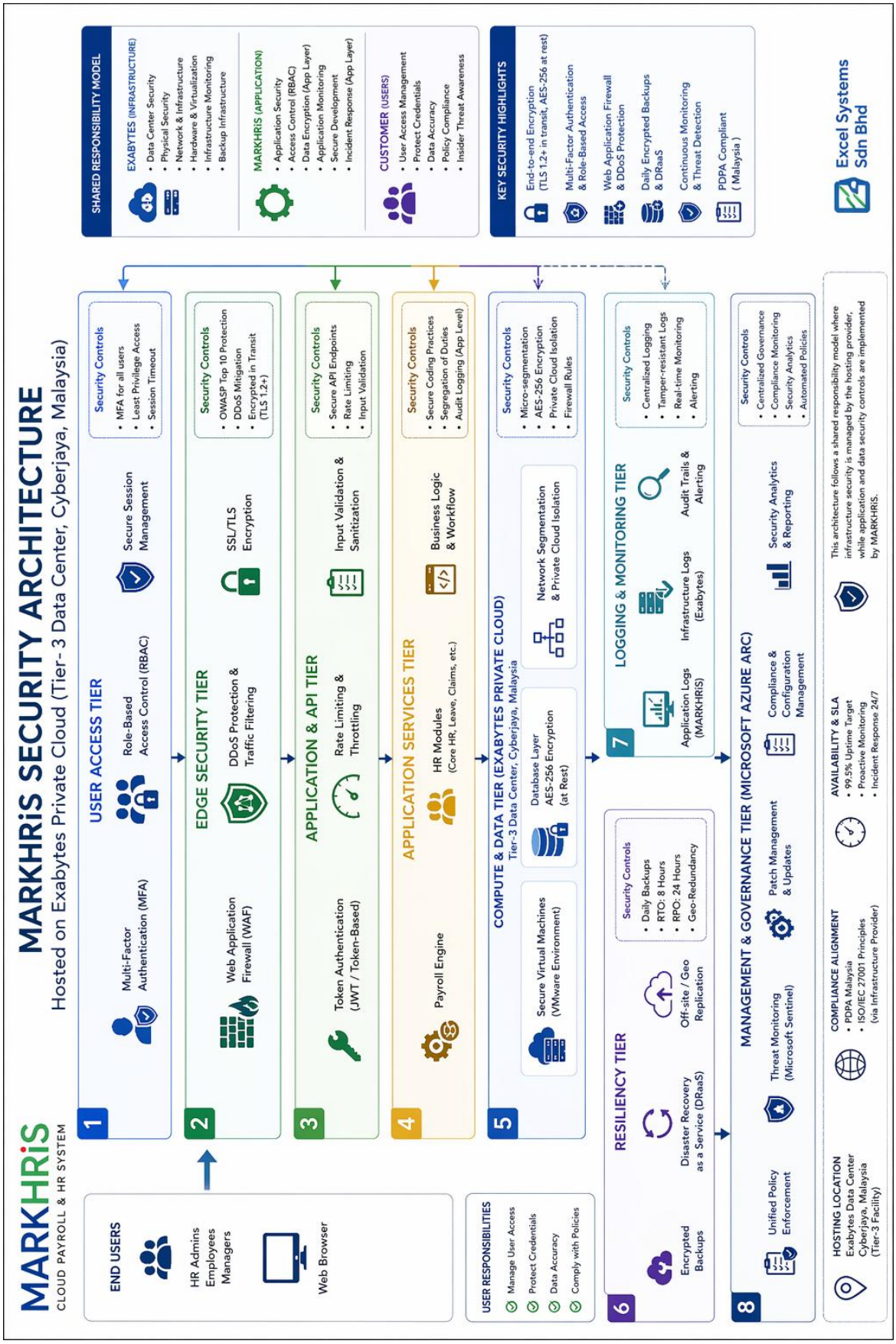
Key Security Highlights

- End-to-end encryption for all data (TLS 1.2+ in transit, AES-256 at rest)
- Role-based access control (RBAC) with strict privilege separation
- Multi-factor authentication (MFA) for enhanced identity protection
- Continuous security monitoring and vulnerability assessments
- Daily encrypted backups with disaster recovery capabilities
- Defined incident response procedures aligned with industry best practices
- Data retention and deletion policies aligned with compliance requirements

Business Assurance

MARKHRiS is designed to support enterprise HR operations while aligning with key regulatory and security frameworks, including the Personal Data Protection Act (PDPA) Malaysia and ISO/IEC 27001 security principles (via infrastructure providers). This ensures that organizations using MARKHRiS can confidently manage sensitive employee and payroll data in a secure, controlled, and auditable environment.

SECURITY ARCHITECTURE OVERVIEW



TECHNICAL SECURITY FRAMEWORK

A. GOVERNANCE & INFRASTRUCTURE

- **Scope:** Applies to all MARKHRiS SaaS modules (Payroll & HR).
- **Security Governance:** Aligned with ISO/IEC 27001; features segregation of duties and formal change management.

B. DATA CENTER & PHYSICAL SECURITY

- **Physical Security:** Hosted in Tier-3 data center in Cyberjaya, Malaysia and managed by ISO/IEC 27001-certified infrastructure provider
- Physical & Environmental Controls
  - Biometric access control
  - CCTV surveillance
  - Fire suppression systems
  - Environmental control systems
  - Redundant power supply (UPS & generators)

C. DATA & IDENTITY PROTECTION

- **Data Classification:** Four-tier model (Public to Highly Confidential). Payroll and Identity data receive "Highly Confidential" status.
- **Encryption Standards:** TLS 1.2+ (In-Transit), AES-256 (At-Rest) and additional application-layer encryption for sensitive financial data.
- **Identity & Access Management:** Role-Based Access Control (RBAC). Multi-Factor Authentication (MFA) supported, and Customer-controlled user provisioning.

D. PASSWORD POLICY

- Minimum length & complexity requirements
- Account lockout after failed attempts
- Password reuse restrictions (configurable)
- Secure irreversible hashing

E. NETWORK & APPLICATION SECURITY

- Web Application Firewall (WAF)
- API token authentication
- Rate limiting and input validation
- Network segmentation

F. THREAT & VULNERABILITY MANAGEMENT

- Quarterly internal vulnerability assessments
- Annual third-party penetration testing
- Continuous patch management

G. LOGGING & MONITORING

Logging and monitoring follow a shared responsibility model:

- Infrastructure-level logging is managed by the hosting provider
- Application-level logging is managed by MARKHRiS

H. BACKUP & DISASTER RECOVERY

- Daily encrypted backups with geographic redundancy. **RTO: 8hrs / RPO: 24hrs.**
- Deleted data may persist in encrypted backup storage for a limited retention cycle before permanent removal.

I. INCIDENT RESPONSE & SECURITY BREACH NOTIFICATION

- Immediate triage and containment
- Investigation and remediation
- Customer notification within 24–72 hours (based on severity)
- Root cause analysis within defined timeframe

J. SHARED RESPONSIBILITY MODEL

MARKHRiS operates under a shared responsibility model to clearly define security accountability between Excel Systems Sdn Bhd (the service provider), its infrastructure partners, and its customers.

This ensures transparency, audit clarity, and alignment with enterprise cloud security standards.

1. Responsibility Overview

Area	MARKHRiS (Excel Systems)	Infrastructure Provider	Customer
Application Security	✓	—	—
Infrastructure Security	—	✓	—
Physical Data Center Security	—	✓	—
Data Encryption (App Layer)	✓	✓	—
User Access Control	Platform	—	✓
Identity Management	✓	—	✓
Logging & Monitoring	Application logs	Infrastructure logs	View access
Vulnerability Management	App layer	Infrastructure layer	—
Backup & DR	Shared	✓	—
Data Accuracy & Usage	—	—	✓

2. Infrastructure Provider Responsibilities

- Physical security of data center
- Server and network infrastructure security
- Hardware maintenance and lifecycle
- Infrastructure-level monitoring and backups

3. MARKHRiS Responsibilities

- Application security design
- Authentication & authorization controls
- Encryption implementation
- Audit logging (application level)
- Security testing and VAPT
- Incident response (application layer)

4. Customer Responsibilities

- User access management
- Data accuracy and integrity
- Internal HR governance
- Credential protection
- Compliance with internal policies

5. **Security Principle**

   This model aligns with industry-standard cloud security frameworks where responsibility is shared across infrastructure, platform, and customer layers.

K. ASSET DISPOSAL

All hardware and storage devices are handled securely throughout their lifecycle:

- Secure data wiping and degaussing before disposal
- Controlled repair and replacement procedures
- Compliance with secure disposal standards

L. COMPLIANCE & COMMITMENT

- **Regulatory Alignment:** Direct alignment with **PDPA 2010 (Malaysia)** and Alignment with ISO/IEC 27001 principles.
- **Service Availability:** 99.5% (excluding planned maintenance)

M. COMPLIANCE DISCLAIMER

MARKHRiS operates on infrastructure certified under ISO/IEC 27001 standards. Excel Systems Sdn Bhd aligns its security practices with these principles but does not claim independent ISO certification unless explicitly stated.

N. COMMITMENT

We are committed to continuously improving our security posture through proactive risk management, infrastructure enhancement, and adherence to industry best practices to ensure the protection of customer data.

APPENDIX

PART 1 — SOC 2 / ISO 27001 CONTROL MAPPING

Note: This control mapping reflects alignment with SOC 2 and ISO/IEC 27001 principles. It does not constitute formal certification unless explicitly stated.

Control Area	SOC Trust Criteria	ISO/IEC27001 Control	MARKHRiS Implementation
Access Control	CC6.1, CC6.2	A.9 Access Control	Role-Based Access Control (RBAC), MFA, least privilege enforcement
User Authentication	CC6.3	A.9.4.2 Secure Log-on	Password policy, account lockout, MFA support
Data Encryption	CC6.7	A.10 Cryptography	TLS 1.2+ (in transit), AES-256 (at rest)
Key Management	CC6.7	A.10.1.2	Encryption keys managed within secure infrastructure (cloud provider controls)
Network Security	CC6.6	A.13 Network Security	WAF, API security, network segmentation
Logging & Monitoring	CC7.2, CC7.3	A.12.4 Logging & Monitoring	Centralized logs, audit trails, activity monitoring
Vulnerability Management	CC7.1	A.12.6 Technical Vulnerability Mgmt	Quarterly internal scans, annual penetration testing
Incident Response	CC7.4	A.16 Incident Management	Defined incident response process, 24–72 hr notification
Backup & Recovery	CC7.3	A.12.3 Backup	Daily encrypted backups, RTO 8h / RPO 24h
Availability	A1.2	A.17 Business Continuity	99.5% uptime target, DRaaS capability
Physical Security	CC6.4	A.11 Physical Security	Tier-3 DC, biometric access, CCTV
Change Management	CC8.1	A.12.1 Change Management	Controlled deployment & patching
Data Retention	P3.1	A.18 Compliance	Defined retention & deletion policy
Data Privacy	P1.1	A.18.1 Compliance	PDPA-aligned processing controls
Security Awareness	CC2.2	A.7 Human Resource Security	Staff training & policy enforcement
Asset Disposal	CC6.5	A.11.2 Equipment Disposal	Secure wiping & degaussing

APPENDIX

PART 2 — SECURITY QUESTIONNAIRE RESPONSE

Category	Question
Data Security	**Q: How is customer data protected?** A: All data is encrypted using TLS 1.2+ during transmission and AES-256 at rest. Additional application-layer encryption is applied to sensitive payroll data.
Access Control	**Q: How do you control user access?** A: MARKHRiS uses Role-Based Access Control (RBAC) with least privilege principles. Customers manage user roles and permissions.
Authentication	**Q: Do you support multi-factor authentication (MFA)?** A: Yes. MFA is supported via authenticator apps or OTP.
Password Policy	Q: What password policies are enforced? A: Configurable policies including: ▪ Minimum length ▪ Complexity requirements ▪ Account lockout after failed attempts ▪ Password expiry and reuse control
Infrastructure Security	**Q: Where is your system hosted?** A: MARKHRiS is hosted in a Tier-3 data center in Cyberjaya, Malaysia, managed by ISO/IEC 27001-certified infrastructure providers.
Network Security	**Q: How do you protect against external threats?** A: ▪ Web Application Firewall (WAF) ▪ API authentication & rate limiting ▪ Network segmentation
Vulnerability Management	**Q: Do you perform security testing?** A: ▪ Quarterly internal vulnerability assessments ▪ Annual third-party penetration testing
Logging & Monitoring	**Q: Do you maintain audit logs?** A: Yes. All critical activities (login, access, changes) are logged and monitored.
Backup & Disaster Recovery	**Q: What is your backup policy?** A: ▪ Daily encrypted backups ▪ RTO: 8 hours ▪ RPO: 24 hours ▪ Geo-redundant storage

Category	Question
Incident Response	**Q: How do you handle security incidents?** A: ▪ Immediate triage and containment ▪ Customer notification within 24–72 hours ▪ Root cause analysis performed
Employee Security	**Q: Do employees receive security training?** A: Yes. All staff undergo onboarding and periodic security awareness training.
Data Disposal	**Q: How is data securely deleted?** A: ▪ Logical deletion after termination ▪ Backup retention expiry ▪ Secure wiping for physical storage
Compliance	**Q: Are you ISO 27001 certified?** A: The hosting infrastructure is ISO 27001 certified. Excel Systems aligns with ISO 27001 principles but is not independently certified unless stated
Data Privacy	**Q: Are you compliant with PDPA?** A: Yes. MARKHRiS aligns with Malaysia Personal Data Protection Act (PDPA) requirements.
Customer Responsibility	**Q: What is the customer responsible for?** A: ▪ User access management ▪ Data accuracy ▪ Internal compliance policies