بسم الله الرحمن الرحيم

TERMS OF REFERENCE

Position:	Head of Infrastructure
Rank / Classification:	Heads of Business Units
Division	Technology, Product and Innovation Division
Duration / Post Type:	Permanent
Reporting Line:	Chief Technology Officer (CTO)

1. Background

The Head of Infrastructure will be responsible for administering, securing, and optimizing Payment Maldives' Microsoft-based infrastructure, including Windows Server, Active Directory, Microsoft Entra ID, Microsoft 365, and endpoint management environments. Operating as a technical specialist, the consultant will ensure seamless identity management, robust endpoint hygiene, and strict access controls across both corporate and regulated payment systems. The role strongly emphasizes proactive security hardening, continuous patch currency, and aligning technical operations with PCI-DSS, ISO 27001, and regulatory compliance standards.

2. Key Responsibilities

- **Windows Server Administration:** Manage Windows Server (2016–2022) lifecycles, core roles (DNS, DHCP, IIS, File Print), failover clustering, storage, and security hardening aligned to CIS Benchmarks.
- **Active Directory & Identity Management:** Govern AD DS architecture, GPOs, tiered administrative privileges, Windows LAPS, gMSAs, AD CS, and automated log integration with central SIEM.
- **Microsoft Entra ID & Hybrid Identity:** Configure hybrid identity sync via Entra Connect, Conditional Access policies, tenant-wide MFA, Privileged Identity Management, and SaaS SSO integration.
- **Microsoft 365 & Collaboration Services:** Administer Exchange Online, SharePoint, OneDrive, and Teams while enforcing email security (SPF, DKIM, DMARC), DLP, and data retention policies.
- **Endpoint Management & Patching:** Deploy Intune/MCM configuration profiles, Autopilot imaging, Defender for Endpoint, BitLocker encryption, and phased patch management cycles meeting remediation SLAs.

- **Backup, Recovery & Business Continuity:** Manage policy-aligned backup schedules, execute verified restore tests, maintain DR procedures for Windows infrastructure and Active Directory, support organizational DR exercises, and ensure strict alignment with RTO and RPO targets.
- **Automation, Security Operations & Compliance:** Automate administrative, reporting, and lifecycle access tasks via a version-controlled PowerShell and Microsoft Graph script library, while ensuring SIEM log integration, vulnerability remediation, immediate incident response, and full PCI-DSS and ISO 27001 audit support.

3. Qualifications & Experience

- Bachelor's degree in computer science, Information Technology, Systems Administration, or a related field. A postgraduate qualification in a related discipline will be an added advantage.
- Relevant Microsoft certifications (AZ-800/801, AZ-104, MS-102, SC-300, MD-102) or ITIL Foundation will be a distinct advantage.
- Minimum 5 years of hands-on experience in production Windows Server and Active Directory administration, Microsoft Entra ID (hybrid sync & Conditional Access), Microsoft 365 (Exchange & SharePoint), Intune/MCM endpoint management, GPO design, PKI/AD CS, Windows security hardening, PowerShell automation and backup/recovery; including at least 3 years of experience in a leadership role.
- Prior experience in a regulated banking, fintech or payments environment will be an added advantage.

4. Deliverables

- **Strategic Assessments & Architecture:** Estate Gap Analysis Report, Active Directory Health & Security Remediation Report, and Documented Identity & Tiered Administration Architecture.
- **Security & Compliance Baselines:** Tenant-wide Conditional Access & Phishing-Resistant MFA Framework, Windows Server/Endpoint Hardening Baselines (including LAPS & BitLocker), and M365 Security & Email Authentication Review.
- **Operational Frameworks & Automation:** Phased Patch Management Framework, Intune Device Compliance Profiles, PowerShell Automation Script Library, and Complete SOP/Runbook Suite.
- **Continuity & Audit Packages**: Verified Backup & Disaster Recovery Test Reports, Quarterly Access Review Reports, and PCI-DSS/ISO 27001 Audit Evidence Packages.

Specific deliverables and timelines may be determined through annual or periodic work plans approved by the CTO.