LADY POHAMBA
private hospital



Head of Information Technology (IT)

Technology leadership, provider governance and service assurance

Job title	Head of Information Technology
Department	Information Technology
Reports to	Chief Executive Officer
Direct report	IT Support Engineer (in-house)
Directs	The outsourced managed-service partner (data centre, infrastructure operations, information security and desktop support) and the hospital's application providers
Location	Lady Pohamba Private Hospital, Windhoek, Namibia
Employment type	Permanent, full-time

PURPOSE OF THE ROLE

Lady Pohamba Private Hospital is a private acute-care hospital in Windhoek with more than 450 staff. Its technology is delivered through a deliberately outsourced model. A managed-service partner provides the data centre, infrastructure operations, information security and desktop support. Specialist providers supply the core applications - currently Trifour (clinical and hospital information system), Sage Evolution (finance), D-Bit (human resources) and Jarrison (time and attendance and access control). One in-house IT Support Engineer provides on-site support.

The Head of Information Technology is the hospital's single accountable executive for technology. The role is that of the informed client: it sets direction, defines what the hospital requires of its providers, holds them to account for delivery, and gives the CEO, Executive Team and Board assurance that clinical and corporate systems are available, secure and fit for purpose. Success is measured by the quality of the service the hospital receives, and the quality of the decisions taken, not by the size of the team managed.

PRIORITIES FOR THE FIRST TWELVE MONTHS

- Establish a baseline of services, contracts, risks and spend, and reset service governance with the managed-service partner.
- Commission an independent assessment of information-security posture and disaster-recovery readiness and agree a funded remediation plan.
- Agree roadmaps, support arrangements and renewal calendars with each application provider.
- Present a three-year IT and digital strategy and budget for approval.

KEY ACCOUNTABILITIES

Managed-Service Partner and Application Provider Governance

- Own the commercial and operational relationship with the managed-service partner: define service scope, service levels, KPIs, reporting, escalation, security obligations, audit rights and continuity requirements, and ensure they are met.
- Direct the hospital's application providers including HIS, Sage, Dbit, Jarrison to name a few - on roadmaps, releases, upgrades, support performance, integrations and licensing, and ensure each application has a named business owner.
- Chair regular service reviews and maintain objective scorecards covering availability, incidents, requests, projects, security, user satisfaction, cost and risk.
- Ensure accountability is clear where an issue spans more than one provider, so that providers resolve it between themselves rather than leaving it to hospital staff.

- Challenge provider recommendations constructively, and verify independently that proposed solutions are necessary, proportionate, secure and commercially sound rather than relying on providers' own reporting.
- Lead selection, onboarding, renewal, re-tendering and exit of providers, and ensure contracts address data ownership, confidentiality, regulatory compliance, subcontractors, portability, transition assistance and termination.
- Manage dependency and concentration risk, with tested contingency and exit plans for provider failure or underperformance.

Technology Strategy and Digital Leadership

- Develop, maintain and present a three-year IT and digital strategy, roadmap and annual operating plan aligned with the hospital's strategy, clinical priorities and risk appetite.
- Advise the CEO, Executive Team and Board on technology opportunities, dependencies, investments, performance and risk, in clear clinical and business language.
- Prepare and manage the IT operating and capital budgets, business cases and investment portfolio, and track the benefits realised.
- Set architecture, integration and data standards so that clinical, finance, HR and access-control systems work together and new solutions fit the existing estate.
- Provide technical governance for digital initiatives, including interoperability, patient-facing services, analytics, automation and responsible use of AI, whether delivered by providers, contractors or in-house, covering design, security and privacy review, testing, operational handover and adoption.
- Work with clinical and business sponsors so that changes are piloted and evaluated, and scaled only where safety, usability and benefit are demonstrated.

Service Delivery and Operations

- Be accountable for the availability, performance and support of clinical and corporate systems, networks, end-user computing and the service desk, with particular focus on clinical areas that operate around the clock.
- Oversee provider-run incident, problem, request, change, release, capacity and asset management. Approve changes that affect clinical systems and confirm that clinical areas are informed, and downtime procedures are in place.
- Act as the senior escalation point for major incidents: declare and coordinate the response, communicate with clinical and executive leadership, and ensure root-cause analysis and corrective action follow.
- Maintain accurate registers of systems, integrations, data flows, licences, contracts, assets and service owners.
- Lead, develop and set objectives for the in-house IT Support Engineer, who is the hospital's on-site presence and first point of contact for users.

Information Security, Risk and Compliance

- Act as the hospital's accountable executive for information security: maintain the strategy, policies, standards and risk register, while the managed-service partner operates the controls.
- Require providers to operate effective controls for identity and access, endpoint protection, patching and vulnerability management, logging and monitoring, encryption and secure configuration, and obtain independent assurance (penetration tests, audits, evidence) that those controls work.
- Coordinate security assessments, audits, remediation plans, staff awareness and incident-response exercises, and lead the hospital's response to cyber incidents and data breaches.
- Ensure technology services meet applicable Namibian legal and regulatory requirements, including data protection and health-records obligations, together with contractual and accreditation requirements (for example COHSASA).
- Report material technology and cyber risks promptly and track treatment actions to closure.

Business Continuity and Disaster Recovery

- Agree recovery objectives with clinical and business owners, and ensure providers maintain documented, tested backup, disaster-recovery and major-incident arrangements so that patient care can continue safely during outages.
- Schedule and witness restoration tests, failover exercises and downtime simulations, and drive the resulting lessons-learned actions.
- Ensure critical dependencies and manual workarounds are documented, and that ward and departmental downtime procedures are current and rehearsed.

Data, Change and Adoption

- Promote data governance covering ownership, quality, classification, retention, access, protection and responsible use, and support reliable management reporting and analytics.
- Lead the change and adoption that accompanies technology: engage stakeholders and frontline teams early, coordinate communication and training, and manage adoption risk.

Financial and Commercial Management

- Control technology expenditure and validate supplier invoices against contracts, consumption, deliverables and service performance.
- Optimise licensing, subscriptions, cloud consumption and asset life cycles to reduce total cost of ownership.
- Lead commercial negotiations with finance, procurement and legal advisers, and maintain transparent forecasts that identify savings without compromising resilience, security or service quality.

AUTHORITY AND DECISION RIGHTS

- Recommend technology strategy, investments, sourcing decisions, policies and risk treatments for executive approval.
- Approve operational changes and expenditure within delegated authority.
- Require corrective action from providers and escalate contractual or security breaches.
- Pause or reject technology changes that create unacceptable operational, security, compliance or financial risk, consulting affected clinical leaders wherever time allows.
- Declare and coordinate major technology incidents under the hospital's incident-response framework.

KEY WORKING RELATIONSHIPS

- **Internal:** CEO and Executive Team; the Board and its relevant committees; medical, nursing and allied-health leaders; finance, HR, procurement, legal, risk and quality; department heads; system owners; and all users.
- **External:** the managed-service partner; application providers; telecommunications and connectivity providers; security specialists; auditors; consultants; and regulators and accreditation bodies.

QUALIFICATIONS AND EXPERIENCE

Essential

- Bachelor's degree (NQF Level 7 or equivalent) in information technology, computer science, information systems, engineering or a related field.
- At least ten years' experience in information technology, including at least five years in a senior management role.
- Demonstrated experience as the client-side head of an outsourced or co-sourced IT environment, holding providers accountable to contracts and service levels, including service reviews, commercial negotiation, renewal and exit.
- Experience leading major-incident response and disaster-recovery testing in an environment where downtime has operational or safety consequences.
- Working knowledge of infrastructure, cloud services, networking, identity, end-user computing, enterprise applications, data protection and cybersecurity, sufficient to challenge providers with credibility.
- Experience of IT budgeting, procurement and executive-level reporting.
- Strong written and verbal communication, with the ability to brief boards, executives and clinicians.

Desirable

- Experience in a hospital or healthcare setting, including clinical information systems and interoperability standards such as HL7 and FHIR.
- Postgraduate qualification (for example MBA or MSc) and/or professional certification such as ITIL, COBIT, CISM, CISSP, CRISC, ISO 27001 or PMP.
- Experience in an accredited or heavily regulated environment, and familiarity with the Namibian and wider SADC technology and connectivity market.

CORE COMPETENCIES

- Strategic thinking and business alignment.
- Supplier governance and commercial judgement.
- Technology and cyber-risk judgement.
- Clear communication with executives and clinicians.
- Negotiation, influence and constructive challenge.
- Calm, decisive leadership during incidents.
- Financial discipline and benefits focus.
- Integrity, accountability and discretion with sensitive patient and business information.

KEY PERFORMANCE INDICATORS

- Targets are agreed with the CEO each year.
- **Service:** availability, response, resolution and user-satisfaction targets met, with particular reference to clinical systems.
- **Providers:** service-level attainment, closure of scorecard actions, and contractual obligations met.
- **Security and resilience:** critical vulnerabilities and audit findings closed on time; recovery tests completed on schedule, with evidence.
- **Delivery:** priority digital initiatives delivered on time and within budget, adopted by users, with benefits demonstrated.
- **Financial control:** IT spend within budget, accurate forecasts, supplier billing validated, and licence and cloud costs controlled.
- **Data and systems quality:** fewer integration failures, less avoidable duplication and reduced technical debt.
- **Governance:** a funded, current roadmap, and timely, decision-useful reporting to the Executive Team and Board.

WORKING CONDITIONS

The role is based on site at the hospital and requires availability outside normal working hours for major incidents, critical changes, disaster-recovery tests and urgent supplier escalations. Occasional travel to provider sites or supplier locations may be required. Appointment is subject to satisfactory reference, qualification and background verification.

Closing date: 06 November 2026

Please submit your CV to **cv@lpph.com.na**

Lady Pohamba Private Hospital · Windhoek, Namibia