Senior Systems Engineer

ROLE TITLE	Senior Systems Engineer
DEPARTMENT	Information Technology
REPORTS TO	Chief Information Officer
DIRECT REPORTS	None; provides technical leadership, mentoring and coordination across internal staff and specialist partners

POSITION OBJECTIVE

The Senior Systems Engineer is the senior operational technical owner for Grand Casino's infrastructure, systems, identity and security services. The role is responsible for maintaining stable, secure, recoverable and supportable production services within a highly regulated gaming and hospitality environment.

Reporting to the Chief Information Officer, the role combines hands-on systems engineering with technical leadership. It establishes and maintains sound engineering standards, strengthens operational resilience and service-management discipline, and ensures internal stakeholders and specialist partners work from accurate technical information.

The role works closely with the CIO, Project Manager / Functional Analyst, It Support Analyst, business managers, vendors, auditors and assurance providers. It contributes technical expertise to investment decisions and change delivery while ensuring new and existing services are safely operationalised.

Role boundary: The Senior Systems Engineer owns technical analysis, execution, evidence and recommended treatment within the role's delegated authority. Technology strategy, investment approval, formal acceptance of organisational risk and executive assurance remain accountable to the CIO or the formally delegated business risk owner.

DELEGATED AUTHORITY

- Approve routine technical and operational actions within documented policies, standards, change authorities and the formal delegated-authority framework.
- Recommend infrastructure, security, licensing and support expenditure to the CIO and manage approved expenditure within any written delegation.
- Initiate urgent containment or recovery action where required to protect safety, gaming integrity, information security or critical service availability, with prompt escalation to the CIO.
- Coordinate technical suppliers and internal resources during incidents and approved changes; commercial commitment and formal risk acceptance remain subject to the appropriate delegation.

KEY ACCOUNTABILITIES

Infrastructure and platform operations

- Operate and improve server, virtualisation, storage, backup, recovery, network, identity, endpoint and cloud platforms within the agreed service ownership model.
- Maintain availability, performance, capacity and configuration baselines for critical systems, proactively identifying constraints and control gaps.
- Ensure patching, certificate renewal, backup, restore testing, lifecycle maintenance and other time-critical activities are planned, completed and evidenced.
- Act as the senior technical escalation point for complex or high-impact infrastructure and systems incidents.

Cybersecurity operations and technology risk

- Lead the implementation and day-to-day operation of security controls across infrastructure, identity, endpoint and network domains.
- Operate controls including multifactor authentication, privileged access, endpoint protection, vulnerability remediation, logging, monitoring and secure configuration.

- Identify and document security exceptions, assess technical risk, recommend treatment options and maintain remediation plans for review by the CIO or relevant risk owner.
- Provide technical evidence for audits, compliance reviews, penetration testing, insurance assurance and regulatory activity.
- Apply recognised frameworks and standards, including the NIST Cybersecurity Framework and Grand Casino's approved security policies and architecture standards.

Identity and access management

- Administer and improve Active Directory, Microsoft Entra ID and related authentication and identity services.
- Maintain privileged-access, break-glass, service-account and credential controls, including appropriate monitoring and periodic review.
- Ensure joiner, mover and leaver processes are timely, standardised, authorised and auditable.
- Work with system and information owners to implement least privilege, segregation of duties and access recertification.

Operational resilience and service management

- Act as the operational technical lead for incident, problem and change management, ensuring technical teams and suppliers follow agreed processes and maintain appropriate records.
- Lead technical diagnosis, containment, recovery and root-cause analysis, including documented follow-up actions and lessons learned.
- Maintain service, asset and configuration information needed to operate, support and recover critical systems.
- Support business continuity and disaster-recovery planning, testing and improvement, with clear recovery objectives and escalation procedures.
- Participate in a formally agreed after-hours support roster with documented handover, escalation, allowance and fatigue-management arrangements.

Monitoring, tooling and automation

- Improve monitoring, alerting, logging, vulnerability management, asset/configuration records and IT service-management tooling.
- Use scripting and automation to improve repeatability, reduce manual effort and strengthen operational control.
- Ensure alerts are actionable, assigned to named owners and supported by documented response procedures.

Vendor and third-party technical management

- Act as the principal technical interface for infrastructure, cloud, security and specialist support partners within the role's service domains.
- Manage technical escalation paths, challenge solution design, validate implementation quality and confirm operational handover requirements are met.
- Monitor technical support performance and contribute evidence and advice to contract reviews, renewals, licensing decisions and supplier-risk assessments.
- Retain internal ownership of architecture, access, configuration standards, service knowledge and risk decisions while using vendors for defined expertise and surge capacity.

Documentation and knowledge ownership

- Own and maintain the authoritative technical operating record for Grand Casino's environment, including architecture diagrams, configuration baselines, asset and service records, support arrangements, SOPs, recovery procedures and dependencies.
- Ensure documentation reflects the operating environment, is version-controlled, periodically reviewed and usable by an appropriately skilled secondary resource.
- Reduce key-person dependency through structured walkthroughs, cross-training, peer review and tested operational procedures.

Projects and controlled change

- Provide technical leadership and delivery support for infrastructure, cybersecurity, platform, application and integration initiatives.
- Support the CIO and Project Manager / Functional Analyst with architecture, requirements, technical risk, estimation, testing and implementation planning.
- Ensure production changes are authorised, peer-reviewed where appropriate, tested, documented, recoverable and transitioned into BAU ownership.
- Confirm monitoring, support, security, licensing, data-flow and recovery requirements are addressed before new services are accepted into operation.

KEY MEASURES OF SUCCESS

- Critical services have named primary and secondary technical owners, current support arrangements and tested escalation paths.
- Scheduled patching, backup, restore testing, certificate renewal, access review and other critical control activities are completed and evidenced within agreed timeframes.
- Critical and high vulnerabilities, audit findings and technical risks are assigned, tracked and treated within approved risk-based targets.
- Recurring incidents are reduced through effective root-cause analysis and completion of problem-management actions.
- Material production changes demonstrate appropriate assessment, testing, approval, implementation evidence and rollback planning.
- Critical SOPs, diagrams, service records and recovery procedures remain current, peer-reviewed and usable by a trained secondary resource.
- Routine external engineering dependency reduces as internal capability, tooling, automation and supplier governance mature.
- Stakeholders receive clear, timely and factual communication during incidents, changes and technical decision-making.

KEY BEHAVIOURS

- **Ownership and delivery:** Takes responsibility through to verified resolution; raises risks early and follows agreed priorities and instructions.
- **Operational discipline:** Prioritises stability, security, evidence and recoverability; works within controlled processes rather than relying on undocumented workarounds.
- **Continuous learning:** Maintains relevant technical knowledge through self-directed learning, certification, peer review, vendor training and practical development plans.
- **Communication:** Communicates clearly and calmly, translates technical issues into business impact and provides evidence-based recommendations.
- **Collaboration:** Shares knowledge, supports secondary coverage, works constructively with colleagues and challenges vendors and stakeholders professionally.
- **Customer focus:** Understands the operational needs of a 24/7 gaming and hospitality business and balances service, security, risk and usability.

TECHNICAL COMPETENCIES

- Strong systems-engineering experience across Windows Server, Hyper-V or comparable enterprise virtualisation, networking, firewalls, storage, backup and recovery.
- Practical expertise with Active Directory, Microsoft Entra ID, Microsoft 365 and contemporary endpoint, identity and security services.
- Hands-on experience implementing cyber controls, secure configuration, vulnerability remediation, privileged-access controls, logging and monitoring.
- Working knowledge of network segmentation, remote access, switching, wireless and firewall policy; Fortinet and Aruba experience is advantageous.
- Experience with disaster recovery, restore assurance, capacity management and the operational support of business-critical applications and interfaces.

- Ability to use PowerShell or equivalent automation and scripting tools to improve control, consistency and efficiency.
- Working knowledge of ITIL-aligned incident, problem, change, configuration, asset and knowledge-management practices.
- Strong analytical troubleshooting, documentation, technical writing and vendor-management capability.

EDUCATION AND EXPERIENCE

- A relevant degree, equivalent professional experience, or a combination of both.
- Approximately eight or more years of systems engineering, infrastructure or senior operational technology experience, including responsibility for production environments.
- Relevant Microsoft, networking, infrastructure, cloud, IT service-management or cybersecurity certifications are desirable.
- Experience in a regulated environment such as gaming, financial services, healthcare or government is advantageous.
- Demonstrated experience supporting audits, assurance activity and the remediation of technology or cybersecurity findings.

TRAINING AND PROFESSIONAL DEVELOPMENT

- Maintain a current professional-development plan aligned with the technologies and services for which the role is accountable.
- Complete mandatory cybersecurity, privacy, health and safety, responsible gambling and other organisational training within required timeframes.
- Maintain sufficient awareness of the Gambling Act 2003, Minimum Operating Standards and related requirements to understand the technology and evidence obligations relevant to the role.

HEALTH AND SAFETY

- Comply with Grand Casino's health and safety policies, immediately report incidents and hazards, and participate in required emergency and evacuation procedures.
- Consider operational safety, data integrity, workload and fatigue risks when planning technical work, after-hours activity and production change.
- Support business continuity, system resilience and safe technology practices across the organisation.

EMPLOYMENT AND REGULATORY REQUIREMENTS

- A current full New Zealand driver licence.
- The legal right to work in New Zealand.
- Appointment and continued employment are subject to satisfying Grand Casino's probity and background-checking requirements and obtaining and maintaining any Department of Internal Affairs Certificate of Approval required for the position.
- Ability to participate in the agreed after-hours support and incident-response roster in accordance with the Employment Agreement and applicable policies.

DECLARATION OF UNDERSTANDING

This Position Description identifies the principal purpose, accountabilities and requirements of the role. It is not intended to be an exhaustive list of every task that may reasonably be required within the scope and seniority of the position.

The duties, accountabilities or Position Description may be reviewed as Grand Casino's legitimate business and technology requirements change. Where a proposed change may materially affect the position or employment arrangements, Grand Casino will consult the employee and follow the applicable employment agreement, policies and legal obligations before making a final decision.

The employee is expected to devote their ordinary working hours and best endeavours to performing the role, comply with lawful and reasonable instructions, and meet the standards contained in the Employment Agreement and Grand Casino policies.

I acknowledge that I have read and understood this Position Description and have had the opportunity to ask questions about its requirements.

Employee name	
Employee signature	
Date	
Manager name	
Manager signature	

Once signed, this Position Description must be retained in the employee's personnel file.