JOB DESCRIPTION

Network & Security Specialist

Purpose

The Network & Security Specialist is a senior role within the Information Technology Department and leads the Business Applications and Quality Assurance Support team.

The role has the following core functions:

1. Assessing, planning and monitoring security measures to protect the organisation's computer systems and network.
2. Developing and publishing Information security procedures and guidelines based on knowledge of best practices and compliance requirements.
3. Overseeing the preparation and execution of required information security policies, procedures, standards, and guidelines.
4. Assist in investigating violations of computer system and network security breaches.

Role Dimensions

Reports to:	Head of Information Technology
Department:	Information Technology
Job Level:	T1
Location:	Head Office, Port Moresby
Direct Reports:	NIL

Person Specifications

- A degree or similar tertiary qualification in Information Technology or similar.
- Proven record of successful experience in information security or related field; experience working within a Finance or Banking organisation being advantageous.
- Well-versed with MS Windows Environment and MS365.
- Experience in generating process documentation & reports.
- Highly proficient technical writing capabilities.
- Good understanding of financing business operation.
- The ability to communicate clearly and precisely with senior level staff including Executive Leadership Team members.
- Adaptable to be flexible in different situations and with all kinds of people.
- Experience in coaching and motivating team members, as well as working well as a team member.

Core Competencies

- Customer service orientated person, with proven success and quality delivery.
- Results orientated person, with proven success and delivery.
- Professional with strong integrity and highly motivated.
- Level-headed, resilient and calm under pressure.
- Ability to deal with ambiguity, have a "can do" work ethic and high energy level.
- Excellent communication skills (written and verbal), delivered with confidence and empathy, necessary to build and develop ongoing and successful relationships with internal clients and third-party service providers.
- Ability to influence and persuade, working across a range of internal clients and stakeholders at various levels of authority.
- Ability to work productively and collaboratively with a diverse and committed group of managers and their teams.
- Familiar with current operating environment and future changes or developments that may impact business.
- Sound interpersonal skills and interpersonal sensitivity.
- Sound planning, organisation and problem-solving capabilities.
- Quality decision making and initiative.
- Understanding of PNG environment or ability to adapt and apply learnings.

Leadership Competencies

- Proven ability to lead by example, motivate, coach and mentor staff to achieve targets whilst remaining empathetic and professional.
- Priority setting and delegation as appropriate.
- Lead and influence others, including those that are not direct reports, managing upwards as necessary.

Role Specific Areas of Responsibility

Operational/	• Assess, plan and monitor security measures to protect FinCorp's computer systems and network. • Develop and publish Information security procedures and guidelines based on knowledge of best practices and compliance requirements. • Monitor endpoint management, patch management, anti-virus management, software updates, incident management, network usage, policy compliance, providing timely and regular update reports. • Capture and monitor any IT incidents/issues, daily by 8.30am (work week), immediately informing the appropriate team/s on any anomalies or situations. • Understand nature of issues, assess turnaround times and how to apply the most appropriate resolution. • Ensure Information Security policies, procedures, standards, and guidelines are written, updated, executed and enforced. • Ensure compliance of relevant regulations and audit findings providing timely and regular update reports on progress. • Perform end-to-end risk assessments, penetration testing and ensure risks are identified and mitigated. • Manage and maintain the ISO27001 certification, reporting on status. • Review violations of computer security procedures. Follow up any violations with the violator and their direct manager to ensure violations are not repeated. • Investigate any non-compliant activities as requested, consulting with the Head of IT, Chief Risk Officer and/or Head of People & Culture, as required. • Prepare IT Risk Reports for the Risk Management Committee, in a timely fashion. • Ensure the issuing of non-compliance to IT Department staff not complying with quality assurance checks for ticket management. • Ensure the issuing of non-compliance to FinCorp staff not complying with Computer Use Policy. • Ensure that all issues are resolved and user requests are managed and delivered within the Service Level Agreements. • Ensure escalated issues to vendor support are resolved within the 3rd Party Service Level Agreements. • Evaluate software alternatives for FinCorp that aim to improve efficiency, communicating requirements clearly with vendors and ensuring solution implementations are within agreed scope, time and cost guidelines. • Ensure monthly reporting to the Head of Information Technology covering but not limited to, Technician non-compliance, ITD SLA breaches & violations, FinCorp staff non-compliance, recurring requests, performance comparisons, recommendation for improvement and identified vulnerabilities and fixes. Quarterly review of user access for all IT systems and networks.
Leadership & Communication	• Lead by example in adhering to Company Policy and procedures, especially when upholding the security and confidentiality of all systems and networks and maintaining compliance of IT policies and processes. • Develop and maintain good working relationships with customers and users. • Coordinate with users on their compliance expectations. • Allocate time to learn and develop skills. • Educate users and promote security awareness and compliance requirements to all FinCorp staff, develop and/or update training materials as required. Training new and existing staff in new system/network functions & procedures, as requested.

	• Regularly distribute 'IT Tips and Techniques' to the business, (minimum of two weeks before every quarter) and more frequent communication as required. • Demonstrate management effectiveness that inspires confidence, promoting teamwork, respect and personal & professional mentoring. • Directly responsible for implementing the ISMS Policy. It is the responsibility of each employee of FinCorp, as well as relevant adjunct business partners, to adhere to the ISMS Policy.