Position Description

Position Title: Platform Support Lead (Infrastructure & Security)

Department: IT Services

Section: Digital Experience & Support

Reports to: Head of Digital Experience & Support

Employment Type: Full-time, Permanent

Position Number: LDL045

Salary Band: Level 1

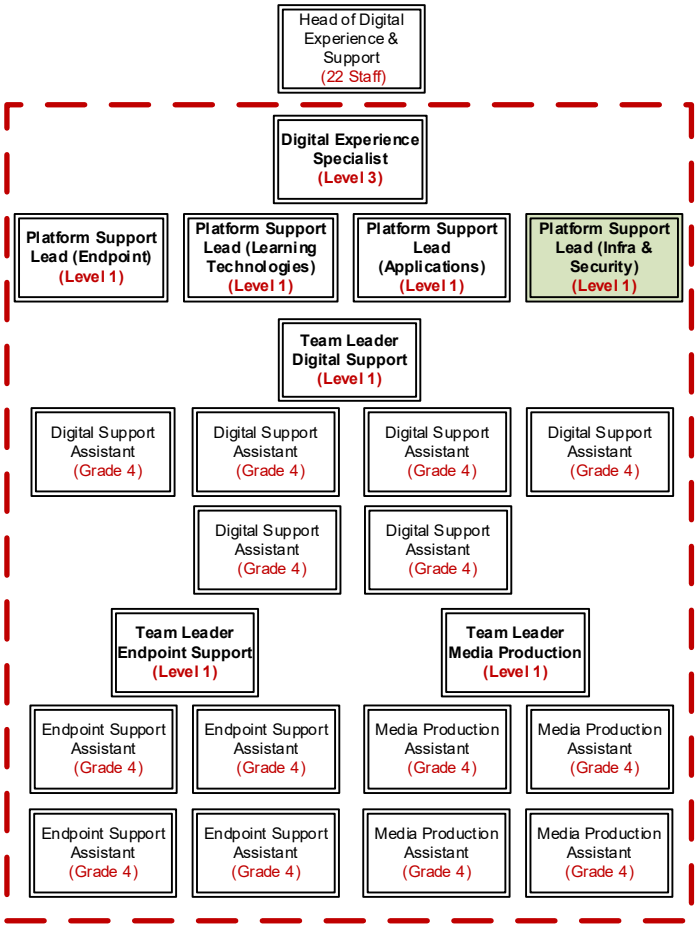
Position Summary

Owns and coordinates support for incidents and service requests that affect stakeholder experience of networks, systems, endpoints and security services. It ensures rapid, clear communication, accurate escalation and effective restoration of service from the user's perspective.

The role bridges technical infrastructure administration with information security operations, ensuring that stakeholders across the region have access to reliable, secure and well-maintained digital infrastructure.

This role also ensures that user impacts are managed professionally, that tickets are properly triaged and progressed and that the security pillars work seamlessly. Includes coordination on digital interfaces to building security systems may be required in collaboration with the Security Services Team.

Structure



Key Responsibilities

1. **NOC / SOC Response & Incident Coordination (35%)**
   - Act as the primary escalation point for infrastructure and security incidents that impact users.
   - Own Tier 2 ticket progression for infrastructure- and security-related user issues: triage, prioritise, communicate status to users, coordinate with Security Engineers and drive resolution or formal handover.
   - Provide clear, timely user communications during major incidents and service degradations, working closely with the relevant security engineers.
   - Maintain situational awareness of active NOC/SOC-style events affecting the user community and the team has accurate information for frontline stakeholders.
   - Support post-incident reviews from a user-impact and service-quality perspective; capture lessons learned that improve future response and communication.
2. **Infrastructure & Support Coordination (25%)**
   - Coordinate infrastructure-related support between support and the cybersecurity team, ensuring clean escalation paths and minimal ticket bounce.
   - Provide Tier 2 technical support for endpoint, access, identity-related and infrastructure issues that can be resolved without deep engineering intervention.
   - Liaise with engineers to progress complex issues while retaining ownership of the user experience and communication.
   - Maintain up-to-date knowledge of services, known issues, maintenance windows and workarounds so that frontline and Tier 2 support can respond effectively.
3. **Service Quality & Documentation (15%)**
   - Develop and maintain support documentation, knowledge-base articles, incident communication templates and quick-reference guides for infrastructure and security-related user issues.
   - Identify recurring user-impacting infrastructure or security issues and recommend service improvements or permanent fixes to the appropriate owners.
   - Ensure support processes for infrastructure and security tickets are clear, measurable and continuously improved.
4. **Coordination with Building / Physical Security (10%)**
   - Collaborate with the Security Services Team on digital interfaces to building security systems (e.g. network connectivity for access control or CCTV, identity integration points) where these affect digital service delivery.
   - Escalate any building-security system faults or operational issues to the correct Security Services owner while supporting any related digital connectivity or identity impacts.
5. **Collaboration & Continuous Improvement (15%)**
   - Work closely with all team members to ensure consistent service standards.
   - Provide regular reporting on infrastructure- and security-related ticket volumes, resolution times, major incidents and user-impact trends.
   - Contribute to service improvement initiatives that enhance the reliability and clarity of infrastructure and security support for stakeholders across all campuses and member countries.

Selection Criteria

Qualifications (or equivalent level of learning)

Essential	*Desirable*
• Bachelor's degree in Information Technology, Computer Science, Cybersecurity, Networking or a closely related discipline. • Minimum 5 years' experience supporting security infrastructure. • Computing Skills - Proficiency in Microsoft Office. • Customer Service & Interpersonal Skills - Strong presentation skills with a demonstrated ability to deliver high-quality customer service and build relationships with diverse stakeholders.	• Exposure within a NOC and SOC environment. • Postgraduate qualification in Learning Technologies or IT. • Networking or security operations (e.g. CompTIA Security+, Network+, ITIL Foundation).

Knowledge / Experience

Essential	*Desirable*
• Solid practical experience in Tier 2 ICT support, incident coordination or service delivery involving networks, systems or security in a multi-site environment. • Working knowledge of enterprise networking, systems administration concepts, endpoint management and common security incident types. • Strong incident communication, stakeholder management and documentation skills; ability to translate technical status into clear user messaging. • Ability to coordinate across technical teams while retaining accountability for user experience and ticket outcomes.	• Experience in higher education or large multi-campus / regional organisations. • Familiarity with NOC/SOC operating models, ITIL incident/problem management and collaboration with specialist engineering teams. • Experience with service management tools, monitoring dashboards, or major-incident communication processes.

Key Relationships / Internal and External Contacts

Lists the key inter-relationships that is necessary for effective performance in the job. Also describe the nature of contact most typically expected with those key working relationships

External	**Purpose of contact**
• Vendors and platform providers	• Technical support escalation, release coordination and product roadmap awareness.
Internal	**Purpose of contact**
• Head of Digital Experience & Support • Digital Security Team • Security Services Team • Stakeholders	• Direction, priorities, service standards, escalation of significant user-impact events and performance feedback. • Technical escalation, joint incident management, clarification of ownership and coordination of user communications during infrastructure or security events. • Consistent Tier 1–2 handling, knowledge sharing and

	coordinated response to user-facing issues. • Coordination on digital interfaces to building security systems only; clear handover of physical security operational issues.

Key Results Area / Key Achievement Areas

Aim: KRAs to have a logical heading. KRAs: 4 – 6.in total Key tasks : 4-5 tasks per KRA. Performance Measures: Identify the performance standards for someone doing the job at the 100% level. Use both quantitative and qualitative measures, Measures the KRA as a whole, not every task. Maximum 3 measures for each KRA Include KRA for Corporate Responsibilities which is generic to all positions

Key Result Areas	***Performance Measures (Jobholder is successful when)***
1. User-Focused Incident Response (NOC/SOC)	• Infrastructure and security incidents affecting users are triaged, communicated and progressed within agreed timescales. • Major-incident user communications are timely and accurate. • Ticket bounce between pillars is minimised.
2. Support Coordination & Escalation Quality	• Clean escalation paths to DI&C are maintained. • Tier 2 infrastructure/security tickets are resolved or formally handed over with full context. • Recurring issues are identified and raised for permanent fix.
3. Service Documentation & Knowledge	• Knowledge-base articles and incident templates for infrastructure/security issues are current and used by support teams. • User-facing guidance is clear and accessible.
4. Security Collaboration	• Effective working relationships with DI&C Principals, Engineers and Security Engineers. • Positive feedback on coordination quality. • Digital-interface issues with Security Services are handled cleanly.
5. Collaboration & Continuous Improvement	• University policies, OHS, equity and code-of-conduct requirements are observed. • Information security and privacy obligations are upheld. • Mandatory training is completed.