Job title:	**Regional IT Infrastructure and Security Engineer**
Directorate:	**IT & Integration**
Date written:	**July 2024**
Notice period:	**3 months**
Job grade:	**GGS**
Job code:	**1676**

Purpose of job

Managing the installation, monitoring, maintenance and support of Abri's back-office IT hardware, software and cloud systems within agreed change of control procedures.

Managing and delivering cost/risk technical projects, upgrades and implementations and provide final escalation technical support to the Group's business users and IT systems.

Assist with the implementation of the organisation's Cyber Security strategy.

Key duties and responsibilities

- Proactively safeguard the IT infrastructure and ensure it is maintained in line with industry best practice and that effective use can be always made of the resources.
- Implementing and maintaining the reliability, availability, scalability and performance of Abri's IT infrastructure through a program of agreed works, ensuring downtime is minimised for customers across all directorates and system up-time is within prescribed SLAs
- Implement security standards, procedures, policies, and guidelines for multiple platforms (including DR and non-production) and diverse system environments based on approved security principles.
- Implement recommended changes from our security team or any internal audits, as needed.
- Ensure all systems, services and platforms are patched in accordance with established patching processes and respond to vendor/3rd party identified security risks in alignment with Cyber Essentials+ timelines.
- Adhere to Abri's change management processes to ensure all changes are logged and managed appropriately.

- Managing technology projects and providing technical resource for high level/risk projects.
- Manage and be accountable for specifically assigned projects and complex technical tasks and the impact they have. Ensure all work is delivered to specification.
- Management and administration of Abri's physical and virtual IT infrastructures, including but not limited to servers, hypervisors, SANs, routers, switches, UPS, LANs, SD-WAN and wireless networks.
- Manage and upkeep of Abri's Azure cloud estate, including AVD and ASR and contribute to the testing of the IT requirements of the Group's business continuity plan.
- Analyse and resolve network, hardware and software problems in a timely and accurate manner and provide end user training where required. Ask questions, apply expertise and research to establish root cause and resolve within timescales and apply remediation afterwards to prevent recurrence.
- Support the IT Service Desk by acting as an escalation point and internal expert on anything Infrastructure or Cyber Security related.
- Apply best practice for installing, configuring, maintaining, and troubleshooting Abri's IT Infrastructure.
- Ensure all systems and infrastructure endpoints are secured in line with Abri's Security Standards within the scope of the role
- Review and remediate all identified IT security risks, understanding the impact they can have on the business and implementing agreed measures to mitigate them.
- Remain current with the latest technologies and solutions. Analyse existing IT infrastructure and IT security landscape and make suggestions for improvement and growth.
- Monitor the usage of the corporate network to ensure compliance with IT security policies, strategies and best practice.
- Liaise with external consultants and service providers to facilitate the provision of IT related systems, which meet the needs of the Group.
- Create and maintain documentation as it relates to any configuration, mapping, processes and service records.
- Carry out any other duties as required for the role.

Knowledge, skills and experience required

- Significant experience in a technical/security role providing escalation type support and ability to troubleshoot complex tasks with a varied toolset such as but not limited to Wireshark and Fiddler.
- A technical qualification such as a Cisco, VMware, CISSP or Microsoft certification.
- An understanding of ITIL with accreditation at Foundation Level.
- Solid understanding of key technologies used by Abri, including Microsoft Windows server technologies, Office365, Azure, VMWare, Enterprise storage, networking and AVD.
- Knowledge of Cloud security environments, standards associated with implementing hybrid on-premise and Cloud solutions.
- Knowledge of industry best practice for security standards and Cloud security standards such as ISO27001, NIST, SANS, CIS, Cloud Security Alliance Cloud Controls Matrix.
- Proven experience of building relationships and managing multi-stakeholder relationships along with the ability to influence, negotiate, generate confidence, trust and respect whilst working (strategically) across a large organisation.
- Effective interpersonal skills, including teamworking and networking skills with the ability to positively motivate all stakeholders, whilst building trusted relationships
- Excellent communication and collaboration skills and a flexible team player personality with a natural ability to work in a rapidly changing environment and multi-task.
- Full driving licence and/or ability to travel in a timely and efficient manner to attend meetings and events in areas not covered by public transport.
- Demonstrates our Values and Behaviours.