INFRASTRUCTURE ENGINEER JOB PROFILE

TITLE	Infrastructure Engineer
POSITION	Member in a team responsible for the building, maintaining and securing the web application infrastructure of the Argentas Platform
UNIT	Information Technology
SUB-UNIT	Systems Development / Back-End Team
DESCRIPTION OF AREA OF RESPONSIBILITY	We are looking for a passionate Infrastructure Engineer to join our team. The Infrastructure Engineer will be responsible for building, maintaining and securing our public facing web application infrastructure including our web applications, decentralized apps (DAPPS) and the primary blockchain testnet. The successful candidate will work closely with the rest of the development team and the Argentas community at large to help build one of the best blockchain eco-systems in the world. The responsibilities of the infrastructure engineer include: • Design and maintain public facing web infrastructure to support Argentas' applications • Ensure uptime of public facing assets • Maintain plans for disaster recovery and business continuity • Maintain security, architecture, and automation of vendor agnostic infrastructure • Establish on-call procedures for infrastructure asset support • Run periodic user access audits, security group audits, and endpoint access audits • Monitor Argentas public asset footprint to minimize recon/profiling from threat actors • Maintain documentation of supported assets for dissemination to teams
REPORTS TO	Back-End Team Lead
DIRECT REPORTS	-
MEMBERSHIPS	Back-End Team
COMPENSATION	Competitive, to be set in connection with the recruitment process
QUALIFICATIONS	• At least 5 years of experience managing infrastructure in a cloud-based environment • Solid understanding of networking fundamentals and theory (IP scope calculating, public vs. private subnets, subnet routing, network ACLs, VLANs, etc.) • Solid understanding of cloud infrastructure fundamentals (public cloud vs. private cloud, tenancy, hotspotting, public endpoints, HA methods, multi-account segmentation, etc.) • Highly experienced with infrastructure security practices (port exposure, ICMP attack mitigation, CORS policy config, DDoS mitigation, etc.) • Highly experienced with administering, maintaining and hardening of multiple flavors of Linux (Amazon, RHEL-like distros, Ubuntu, etc.) • Intermediate experience with software VPN technologies in multiple configurations (client access, site-to-site tunneling, NIC tunnel mesh) • Understanding of blockchain theory and technologies