For Immediate Hiring

The ***Policy Coordination and Monitoring Division (PCMD)*** of the Philippine Council for Industry, Energy, Emerging Technology Research, and Development (PCIEERD) is looking for a result-driven, analytical, detail-oriented, and resourceful individual to fill the vacancy for:

Project Technical Specialist I – Security Specialist
Contract of Service
SG 16 (Php 47, 606.00/mo)

Qualifications:

- Must be a BS Degree holder in Computer Science, Information Technology, Computer Engineering, or any related courses;
- Must have a minimum of two (2) years of relevant technical experience in network administration; With at least sixteen (16) hours of relevant training;
- With experience in handling Active Directory, Azure Active Directory, Office 365 Administrator, Network Switches, Router, Firewall, Cloud Virtual Machine, Virtual Private Network, Web servers, and VOIP Services;
- Knowledge/experience in ISO 27001 Information Security Management System (ISMS) audits and implementation is a plus factor;
- Certification in Cisco, Microsoft, Juniper, CompTia, ITIL, Virtualization, Cloud Computing, CCNP, CCNA, SIEM, CISA, etc., is an advantage;
- Knowledge of best practices around management, control, monitoring, and securing server/network infrastructure;
- Knowledgeable in operational and procedural aspects of computer system, hardware, software, and peripheral equipment;
- Familiarity with backup and recovery software and methodologies;
- Ability to resolve customer complaints/concerns and communicate technical information to technical and non-technical personnel.

Job Description:

- Recommends, develops, designs, and implements, comprehensive IT network security infrastructure solutions/architectures, plans, policies, program, procedures, and measures for maintaining the confidentiality, integrity, and availability of the Council's ICT infrastructure and implementing the Information Security Management System (ISMS);

- Secures network infrastructure and operations (firewalls, proxies, content filtering, load balancers, VPN gateways, IDS, IPS), enforcing standards, policy compliance and running day-today operations;
- Develops, maintains and improves existing/ new security technologies, processes, and governance to affect a proactive security monitoring/ detection capability;
- Enforces security governance by monitoring and administering security technologies (IPS/IDS, firewalls, DDoS Protection, Anti-Virus, Server Patching, Web-Filtering, NAC, Data Loss Prevention, Proxy, and E-mail filtering, identify management system and tokenization;
- Gathers and understands network security requirements, controls, policies, and threats by consulting with other internal security experts, 3rd party sources, and suppliers on current and future threats, mitigations, and services;
- Takes lead in the identification of opportunities and development of recommendations to eliminate risk, improve service capability, and reduce cost;
- Supplies thought leadership regarding network security hardware and software technologies and infrastructure architecture;
- Provides support to the production environment and ensures that the standard security policies and practices are implemented and enforced, including conducting client penetration and vulnerability tests and reports;
- Manages, installs, and configures servers, local area network, wireless infrastructure, and cloud computing services, assisting in maintaining the operating system and security software used on the network, and executing preventive maintenance to enhance network availability;
- Takes part in the preparation of the Council's 3-year Information System Strategic Plan (ISSP) in terms of network-related concerns (i.e., network layouts, ICT Hardware and Software requirements, network projects);
- Prepares and evaluates network-related procurements;
- Contributes to specialized IT project development activities;
- Administers and enforces controls on the following areas: physical, hardware, software, recovery, and backup. Monitors and troubleshoots system software and hardware, and internet and network usage to improve performance and ensure compliance with security policies and standards;
- Collaborates with other teams in the organization as a technical resource in all technical matters, such as educating/training about security software and best practices, and replying to clients on issues ranging from features, and functionality to integration, specifications, and installation;
- Performs other duties of a regular or special nature as assigned.

Competencies:

- **Core Competencies**: Delivering Service Excellence; Promotion Innovation; Exemplifying Integrity;
- **Functional Competencies:** Planning, Organizing and Programming; Building Collaborative Working Relationships; Communicating Effectively; Managing Records and Information; Analytical Thinking and Decision Making.
- **Technical Competencies**: Policy Development and Research Review; Project & Program Development Management; Performance Management; Project Viability and Sustainability; Applying Technical Expertise; IT Resource Management; Risk Assessment.

PCIEERD encourages interested applicants including persons with disability (PWD), members of the indigenous communities and any sexual orientation and gender identities to submit scanned/soft copies of the following documents to **hr@pcieerd.dost.gov.ph** on or before **April 26, 2024;**

- Fully accomplished Personal Data Sheet (PDS; CSC Form No. 212, Revised 2017) which can be downloaded at www.csc.gov.ph;
- Performance rating in the last rating period;
- Certificate of Eligibility/rating/license, if applicable;
- Transcript of Records and Diploma;
- Summary of trainings/seminars/workshops attended;
- Updated Resume; and
- Application Letter addressed to:

DR. ENRICO C. PARINGIT
Executive Director

Please indicate the position, division and posting number **(PTS I – Security Specialist-PCMD-24-24)** as the subject of your email. Qualified applicants will be contacted, so please check your e-mail, and keep your lines open. ***Applications with incomplete documents will not be processed.***