JOB DESCRIPTION
GREENEVILLE ENERGY AUTHORITY

POSITION: **IT Engineer II**

Reports to: Director of Information Technology
Date: 12/02/2025
Approved: Director of Information Technology

Department: Information Technology
FLSA Status: Exempt
Pay Status: Salary

SUMMARY OF DUTIES AND RESPONSIBILITIES

General IT Responsibilities

- Administer, maintain, and support a wide range of IT systems, including servers, workstations, network infrastructure, cloud services, and mobile devices
- Provide technical support to end-users via in-person, remote, and phone support channels
- Troubleshoot hardware, software, and network issues to ensure minimal downtime and operational efficiency
- Install, configure, and manage system updates, patches, and software applications across the organization
- Support and manage enterprise software platforms such as Microsoft 365, Active Directory, and virtualization environments
- Assist with backup, disaster recovery planning, and routine system maintenance
- Participate in IT projects across departments, including upgrades, migrations, and new technology implementations
- Perform other duties as assigned by the Director of IT

Cybersecurity Responsibilities

- Design, implement, and maintain security controls across systems, networks, and user environments
- Monitor systems for threats and respond to incidents using industry-standard tools (SIEM, IDS/IPS, endpoint protection, etc.)
- Develop and maintain IT security policies, procedures, and compliance standards (e.g., NIST, NERC CIP, ISO 27001)
- Deliver cybersecurity awareness training to staff and provide security guidance as needed
- Investigate security incidents and recommend/implement corrective actions
- Stay current on emerging threats, technologies, and best practices in cybersecurity

REQUIRED OPERATION OF EQUIPMENT / OFFICE MACHINES

- Security monitoring systems, SIEM platforms, vulnerability scanners, penetration testing tools
- Network security appliances (firewalls, IDS/IPS, NAC systems)
- Microsoft and Linux operating systems, virtualization platforms, cloud environments
- Personal computers, servers, network equipment, SCADA security systems, terminals, and control units

EDUCATION REQUIREMENTS

- Bachelor's degree in Cybersecurity, Information Security, Computer Science, or equivalent experience/certifications
- Industry certifications preferred: CISSP, CEH, Security+, or similar
- High School diploma or equivalent

SPECIAL SKILLS AND TRAINING REQUIRED

- 5+ years of experience in information security, cybersecurity, or related field
- Knowledge of security frameworks (NIS, ISO, NERC CIP) and regulatory compliance
- Experience with security tools: SIEM platforms, vulnerability scanners, penetration testing tools, endpoint protection
- Strong knowledge of network security protocols, encryption technologies, and secure network architecture
- Scripting capabilities (PowerShell, Python, Bash) a plus
- Strong problem-solving and communication skills
- Ability to work independently and collaboratively across departments
- Ability to stay current with emerging cybersecurity threats and technologies

WORK ENVIRONMENT AND PHYSICAL REQUIREMENTS

- Predominantly office work with occasional fieldwork
- May require 24/7 on-call availability for security incident response
- Periodically work extended hours during security incidents, system implementations, or maintenance windows
- Ability to lift office and IT equipment as needed

SUPERVISORY RESPONSIBILITIES

- No direct supervisory responsibilities
- May provide guidance and mentoring to IT staff

ASSET RESPONSIBILITY

- Responsible for securing and maintaining critical IT infrastructure and data
- Responsible for maintaining the security posture of utility operations and customer data

FREQUENCY AND NATURE OF BUSINESS CONTACTS

- Regular contact with vendors, consultants, and external IT/security professionals
- Coordination with law enforcement and regulatory bodies during security incidents
- Participation in utility industry security forums and threat intelligence sharing group

FREQUENCY AND NATURE OF CUSTOMER CONTACTS

- Minimal direct customer contact
- May interact with customers during security-related service impacts or communications
- Demonstrates strong communication and interpersonal skills to effectively collaborate with internal customers, including technical and non-technical stakeholders. Translates complex technical issues into clear, user-friendly language to ensure timely issue resolution, promote user understanding, and support organizational goals.

ADDITIONAL NOTES

- Must be a self-starter and take initiative to improve systems throughout all departments
- Must maintain confidentiality regarding sensitive IT and security data
- Expected to remain current on trends in IT and cybersecurity

---

_____ _____

EMPLOYEE SIGNATURE DATE

_____ _____

SUPERVISOR SIGNATURE PRESIDENT & CEO