Job Description

Information/Cyber Security Specialist

Description

Reporting to the Chief Information Officer, the Cyber Security Specialist is responsible for overseeing the security of the business environment, including the implementation of security controls and auditing existing systems. The InfoSec Specialist is also responsible for establishing policies and procedures to protect the company and Planned Parenthood data and systems. The Cyber Security Specialist is expected to work closely with the infrastructure team to ensure that existing and new systems are de-signed to meet required security controls. The Cyber Security Specialist will also work with teams across the company to solicit their involvement in achieving higher levels of security through information sharing and cooperation.

Requirements

Essential Functions

- Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.
- Collaborate with information technology staff to design and implement disaster recovery plan for operating systems, databases, networks, servers, and software applications with an emphasis on security.
- Manage all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
- Maintain up-to-date knowledge of the IT security industry, including awareness of new or revised security solutions, improved security processes and the development of new attacks, and threat vectors.
- Supervise all investigations into anomalous activity and provide ongoing communication with senior management.
- Routinely perform security self-assessments of the The Company environments.
- Attest to the function of the information security controls on, at minimum, a quarterly basis.
- Manage special information security projects such as planning upgrades, enhancements, and testing.
- Ensure systems security and integrity of The Company and Planned Parenthood data complies with federal, state, and local laws.
- Perform routine vulnerability assessments and coordinate resolution of identified risks or issues with the relevant parties.
- Work closely with the MSSP in day-to-day SOC operations and SIEM oversight.
- Manage security audits and logs; generate reports as requested.

- Perform regular security awareness training for all employees to ensure consistently high levels of compliance with policies and procedures.

Values and Commitments

- Commitment to Planned Parenthood's mission and conviction about bodily autonomy and health equity.
- Understanding of racism and commitment to racial equity.
- Awareness of multiple group identities and their dynamics, bringing a high level of self-awareness, empathy, and humility to interpersonal interactions.
- Effective interactions and building of trust across diverse groups of people.
- Demonstrated ability to communicate and hear effectively across differences and reflect and act on feedback related to identity and equity with the aim to learn.
- Commitment to Planned Parenthood's In This Together service ethos, workplace values, and service standards

Qualifications, Experience, and Certifications

Required

- Experience in compliance requirements and industry standards such as PCI, HIPAA, and NIST.
- Experience with administering Linux and Windows systems.
- Experience with SIEM, vulnerability scanning, and penetration testing systems.
- Knowledge of computer networking concepts and protocols (e.g., TCP/IP, DNS) and network security methodologies (e.g., Kerberos, SSL/TLS)
- Knowledge of application firewall concepts and functions (e.g., DLP scanning and Web Application Firewalls).
- Extensive knowledge regarding security threat and attack countermeasures.
- Knowledge of business continuity and disaster recovery operation plans.
- Knowledge of identity and access management methods.
- Experience with information security best practices for cloud and on-premise networks.
- Ability to communicate effectively and unambiguously with all levels of staff, stakeholders, and vendors.
- Ability to lead initiatives and manage them independently and with professional discretion.
- Ability to interact with multiple vendors to achieve integrated solutions.
- Ability to ensure a racial equity lens is used when contracting with vendors.
- Ability to work days, evenings, and weekends as required.
- Ability to respond to urgent situations during nonstandard hours with short or no notice.
- Demonstrated history of strong customer service to diverse internal and external stakeholders.
- Ability work in a team environment and maintain confidentiality.
- Ability to run troubleshooting sessions and present the root cause and solution to upper management and leadership.
- Ability to quickly identify and escalate (as needed) issues.
- Excellent problem-solving skills.

- Excellent management and time-management skills.

Preferred

- Experience with AWS.
- Experience with Epic or other electronic health record systems.
- Ability to prepare and deliver presentations to and educate nontechnical stakeholders on network architecture, issues, and roadmap.
- Any relevant security certifications, preferably CISSP, or CISM.