Information Security Supervisor Job

Employer Name:

SpiderID: 12488514

Location: Billings, Montana

Date Posted: 5/3/2022

Wage: Negotiable

Category: Information Technology

Job Code: req3507

Information Security Supervisor  
  
 IT TECHNICAL - 8736 (Billings Clinic Main Campus)  
  
 req3507  
  
   
  
 Shift:Day  
  
 Employment Status: Full-Time (.75 or greater)  
  
 Hours per Pay Period:1.00 = 80 hours (Exempt)  
  
 Starting Wage DOE  
  
   
  
This Position could be performed remotely if residing in the states of Montana, Wyoming, Hawaii, Kansas, Minnesota, or Texas.  
  
The Information Security Supervisor will have responsibility for an assigned group of staff who support providers at Billings Clinic and its affiliates and fulfill a provider support role. Accountabilities include quality of services delivered; short and long-term planning to achieve goals and objectives; provider, interdepartmental and intradepartmental relationships. The Information Security Supervisor responsibilities include performing system build and maintenance; project leadership and participation in multidisciplinary team settings; onboarding and ongoing education; departmental rounding; maintaining a high degree of contact with staff to respond quickly to their changing needs; managing customer satisfaction and maintaining high service levels. This position plays a strategic role in communicating changes in processes and procedures to staff, Information Technology staff and employees in a clear and timely manner. Advocates for standardization and optimization that promotes efficient staff workflows and continually seeks opportunities for innovations with new technology advancements. Additional supervisor responsibilities related to daily operations include timesheets, coordination of on-boarding new staff, resource allocation and prioritization, develops reporting measures for support activity, coaching/counseling, staff evaluations, and acts as a liaison to senior leadership as well as affiliate and/or managed and non-managed sites.  
  
Essential Job Functions  
  
Support and model behaviors consistent with Billings Clinic's mission, vision, values, code of business conduct and service expectations. Meets all mandatory organizational and departmental requirements. Maintains competency in all organizational, departmental and outside agency standards as it relates to the environment, employee, patient safety or job performance. Utilizes process improvement principles to assess and improve provider workflows with a constant view towards workflow improvements and provider satisfaction.  
  
 \* Demonstrates and encourages an ethic of open communication and teamwork throughout the organization. Builds an environment of shared commitment to Billings Clinic's goals and responsibility to achieve quality outcomes. Provides consultation for related concerns and acts as a customer advocate by demonstrating sensitivity to ethical and legal ramifications of practice.  
  
 \* Participates in and provides feedback into the functions of interviewing, hiring, scheduling, mentoring, coaching/counseling, disciplinary actions and terminations as coordinated with IT leadership and Human Resources. Adheres to administrative policies and procedures relating to human resource management.  
  
 \* Ensure team adherence to all organizational and IT processes, policies and procedures.  
  
 \* Works in alignment with project management teams on the coordination of related team resources and capacity for upcoming projects for the organization.  
  
 \* Lead large cross-functional teams and projects to ensure integration of new business initiatives within processes and systems.  
  
 \* Build and maintain relationships with providers, staff, leadership, and vendors to better understand and anticipate their objectives, needs and expectations. Acts as a single point of contact for bi-directional communications between providers and the organization related to system activities and issues pertaining to the provider workflows.  
  
 \* Provide front line cybersecurity support for Billings Clinic and as needed support for affiliate and/or managed and non-managed sites.  
  
 \* Work with external vendors and internal staff/teams within Billings Clinic to ensure system confidentiality, integrity, and availability to meet business needs. Serves as internal or external escalation contact.  
  
 \* Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.  
  
 \* Advise senior management (e.g., Chief Information Security Officer [CISO]) on risk levels and security posture.  
  
 \* Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.  
  
 \* Collect and maintain data needed to meet system cybersecurity reporting.  
  
 \* Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.  
  
 \* Ensure that security improvement actions are evaluated, validated, and implemented as required.  
  
 \* Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.  
  
 \* Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).  
  
 \* Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.  
  
 \* Identify alternative information security strategies to address organizational security objective.  
  
 \* Identify information technology (IT) security program implications of new technologies or technology upgrades.  
  
 \* Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.  
  
 \* Manage the monitoring of information security data sources to maintain organizational situational awareness.  
  
 \* Participate in an information security risk assessment during the Security Assessment and Authorization process.  
  
 \* Participate in the development or modification of the computer environment cybersecurity program plans and requirements.  
  
 \* Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.  
  
 \* Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.  
  
 \* Recognize a possible security violation and take appropriate action to report the incident, as required.  
  
 \* Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.  
  
 \* Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.  
  
 \* Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.  
  
 \* Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.  
  
 \* Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.  
  
 \* Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.  
  
 \* Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.  
  
 \* Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.  
  
 \* Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).  
  
 \* Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.  
  
 \* Performs other duties as assigned or needed to meet the needs of the department/organization.  
  
Knowledge of:  
  
Knowledge of data backup and recovery.  
  
 \* Knowledge of business continuity and disaster recovery continuity of operations plans.  
  
 \* Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.  
  
 \* Knowledge of controls related to the use, processing, storage, and transmission of data.  
  
 \* Knowledge of COBIT, NIST, OCTAVE, and/or ISO frameworks  
  
 \* Knowledge of encryption algorithms.  
  
 \* Knowledge of the organization's enterprise information technology (IT) goals and objectives.  
  
 \* Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).  
  
 \* Knowledge of measures or indicators of system performance and availability.  
  
 \* Knowledge of regulations, laws, policies, procedures, or governance relevant to cybersecurity  
  
 \* Knowledge of PCI DSS, HIPAA, and confidentiality requirements  
  
 \* Knowledge of network traffic analysis methods.  
  
 \* Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.  
  
 \* Knowledge of server and client operating systems.  
  
 \* Knowledge of identity and access management  
  
 \* Knowledge of zero-trust, least-privileges, and role-based access (RBAC)  
  
 \* Knowledge of new and emerging information technology (IT) and cybersecurity technologies.  
  
 \* Knowledge of current and emerging threats/threat vectors.  
  
 \* Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).  
  
 \* Knowledge of system and application security threats and vulnerabilities (e.g., SQL injection, buffer overflow, mobile code, cross-site scripting).  
  
 \* Knowledge of penetration testing principles, tools, and techniques.  
  
 \* Knowledge of SaaS, IaaS, PaaS, and other cloud services  
  
Minimum Qualifications  
  
 Education  
  
Bachelor's Degree in Information Assurance, Information Technology, Computer Science or related field. Graduate degree preferred.  
  
Experience  
  
Five to ten years experience in information assurance, information security, computer science or related field required  
  
 \* Demonstrated management/leadership and program management skills related to the above tasks, knowledge, skills, and abilities  
  
 \* Health Care experience preferred  
  
 \* Functional knowledge of Healthcare EMRs,  
  
 \* Formal project management experience preferred  
  
Certifications and Licenses  
  
CompTIA Security+, EC-Council CEH, GIAC GSEC, or similar at hire  
  
 \* CISSP, CISM, or similar within 1 year of hire  
  
 \* Current Montana/Wyoming driver's license and the ability to be insured to operate Billings Clinic vehicles at hire

Start Date:   
  
  
Position Type: Full-Time Permanent  
  
  
Years of Experience Required:   
  
  
Education Required:   
  
  
Overnight Travel:   
  
  
Vacation Time:

Contact Name: Billings Clinic

Company: Billings Clinic