Position #315271
IS Technical Services Consultant/Administrator
Cybersecurity Engineer Lead Worker
DTSDS/BISM

POSITION SUMMARY

Under the general supervision of the Chief Information Security Officer (CISO) in the Bureau of Information Security Management (BISM) this position provides the Department of Employee Trust Funds (ETF) with the highest level, expert professional information security work including full-spectrum technical design, implementation, and maintenance of security controls for all aspects of ETF's information technology enterprise. This also includes systems and services hosted by the Wisconsin Department of Administration (DOA) Department of Enterprise Technology (DET) as well as cloud hosted services or infrastructure.

This position serves as the principal security technical advisor to the ETF CISO to ensure that ETF successfully manages information security risk. As the team lead, this position leads technical initiatives and selects and implements tools and processes designed to detect, validate, contain, and remediate cyber threats. To that end, the incumbent provides technical expertise and support in the development and implementation of security controls designed to develop a defensive cyber security posture. This position will support ETF's information security strategy and manages technical security projects for the development, testing, and implementation of ETF's major platforms in the application portfolio.

This position requires the incumbent to develop, maintain, and optimize collaborative relationships with cross-functional project teams, DET business and infrastructure teams, contractors, and vendors. The incumbent provides technical expertise for the development of information security policy, standards, procedures, and guidelines. The incumbent performs security administration tasks, as directed. The incumbent may also serve as a representative of the CISO at committees, meetings, and other forums.

ETF is a medium sized, non-shared services agency administering the Wisconsin Retirement System and related benefit programs to over 630,000 members receiving $5.6 billion in retirement benefits and $1.6 billion in health benefits annually. This position directly supports the agency strategic goal focused on building a talented and agile workforce necessary for achieving the department's mission to develop and deliver quality benefits and services to our members while safeguarding the integrity of the Trust. As an employee of ETF, the incumbent will support and create a diverse and inclusive work force.

GOALS AND WORKER ACTIVITIES

40% GOAL A: Provision of project management, technical expertise, and leadership for security-related projects

A1. Direct technical design projects to develop and implement information security controls that protect ETF data across all platforms.

A2. Direct projects to research, select, plan for, install, configure, operationalize, and maintain information security controls for ETF's enterprise-wide business solution application software.

A3. Function as the principal security expert and provide technical direction and operational leadership to cross-functional project teams assigned to deliver security-related solutions, products, and services.

A4. Lead and advise project team members in the installation, configuration, monitoring, validation, and remediation of cyber incidents.

A5. Direct the completion of project tasks to ensure timely, accurate, and quality delivery.

A6. Provide project status and completion reports to the CISO.

A7. Work with the CISO to develop information security-related strategic, tactical, and operational project plans.

A8. Work with service providers to oversee the secure installation, configuration, operation, and maintenance of ETF infrastructure and services.

35% GOAL B: Provision of technical expertise and leadership for BISM

B1. Serve as the team lead for BISM's technical planning, research, and integration of security-related improvements to ETF enterprise applications and infrastructure systems.

B2. Provide technical expertise, direction, and leadership to BISM technical staff. Provide information security-related support for ETF application and infrastructure issues.

B3. Define, research, and recommend the selection of and integration of technical security controls to protect ETF data.

B4. Coordinate internal, state, and vendor-provided technical risk assessments of ETF infrastructure and applications. Evaluate the results and propose solutions.

B5. Coordinate, lead, and direct BISM and other personnel in all aspects of ETF's technical and forensic response to information security incidents. Provide accurate, timely, and quality technical and forensic information to ETF's strategic incident response team and other incident response teams.

B6. Provide consultation to the CISO and other ETF stakeholders to ensure ETF's information security-related systems are an integral part of the ETF Continuity of Operations Plan (COOP).

B7. Coordinate maintenance of change management documentation for information security-related systems.

B8. Provide domain administrator support to Bureau of Information Technology Services (BITS) when needed.

B9. Direct teams in the installation, configuration, and testing of endpoint hardware, software, network, and security software.

B10. Direct teams in the installation, configuration, and testing of networked peripheral hardware (e.g., printers, scanners, etc.).

B11. Direct teams in the planning and implementation of network configuration changes, including testing and roll-back planning.

15% GOAL C: Development, administration, and maintenance of information security standards and procedures

C1. Collaborate with BITS personnel to ensure BITS operations comply with information security principles, policy, standards, and procedures.

C2. Collaborate with internal and external stakeholders to develop and administer standards, procedures, training, and best practices that supports ETF's information security strategy.

C3. Develop information security-related procedures for the continuous monitoring of ETF's business application platforms such as the insurance administration system.

C4. Collaborate with the ETF Office of Communications to ensure effective messaging about security standards and procedures to the ETF user community and other relevant stakeholders.

C5. Work with the CISO to develop, implement, and periodically test ETF's Incident Response Plan.

10% GOAL D: Performance of other duties as assigned

D1. Work with other BITS staff on new and developing technologies and assess their impact on agency system security.

D2. Read articles and other resources and attend training sessions and workshops to improve knowledge of information security and system design principles.

D3. Read security reports published by various public and private organizations, to stay current on newly discovered computer security vulnerabilities.

D4. Maintain knowledge and an ongoing awareness of Department values. Actively embrace the Department's values and fully incorporate them into all aspects of job performance and customer service interactions.

D5. Represent ETF IS interests and/or act as representative of CISO at state committees, meetings, conferences, or other forums, as directed.

D6. Work with the CISO to plan, budget, and operationalize information security efforts across ETF's enterprise.

D7. Provide metrics and other output from information security-related systems and processes to CISO and ETF leadership as requested.

D8. Perform other duties as assigned.

KNOWLEDGE, SKILLS, AND ABILITIES

KNOWLEDGE OF:

1. Security software and configurations specific to Windows desktop, server operating systems, and software products (e.g., Microsoft Office and Microsoft Active Directory)
2. Security software and configurations specific to end points, network hardware, and software
3. Security technology standards (i.e.- NIST, SANS, CIS, OWASP, ISO, etc.) and their application to enterprise environments
4. Computer systems and programs unique to the Department of Employee Trust Funds
5. Security-related Linux distributions and their system and network penetration toolsets (e.g., Kali, BlackBox, etc.)
6. Department's technical and business area programs, processes, and requirements
7. Social engineering and leadership techniques and methods

SKILLED IN:

8. Selecting, implementing, and maintaining security-related systems across multiple platforms and applications software
9. Developing, administering, maintaining, and documenting information security processes and best practices
10. Operating system and productivity software configuration hardening frameworks such as NIST, SANS, CIS, OWASP, ISO, or similar
11. Selecting, implementing, configurating, and maintaining automated software distribution and patching systems, Cisco switches, routers, and firewalls
12. Using the following security tools: vulnerability scanning tools such as Qualys and Nessus; SIEM tools such as QRadar, Splunk, and SolarWinds LEM; anti-malware tools such as Symantec, Norton, and McAfee; and web filter tools such as ZScaler, Forcepoint, and Bluecoat.

ABILITY TO:

13. Direct and lead the work of IT professionals and project teams
14. Work independently and as part of a team
15. Lead information security projects
16. Communicate technical information effectively in plain language, either orally or in writing, to various levels of stakeholders
17. Analyze complex system problems and developing solutions
18. Collaborate with a variety of persons at technical, consultant, and manager levels
19. Prioritize tasks, organize complex information, and manage time effectively
20. Adapt and adjust to changes in technology, processes, and priorities
21. Provide expertise and problem resolution across multiple platforms and software

22. Take initiative to assertively represent business needs. Stand firm when necessary and compromise when possible. Diplomatically challenge assumptions and make recommendations to business and technical staff at all levels of responsibility and authority throughout the department.
23. Understand and comply with all ETF and enterprise security standards, policies, processes, and procedures
24. Maintain confidential information in accordance with policies, guidelines, and direction from manager