**Position #315271**
**IS Technical Services Consultant/Administrator**
**Information Security Lead Worker**
**DMS/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 expert professional-level information security work including; full-spectrum technical design, implementation, and maintenance of security controls for all aspects of ETF's information technology enterprise, including those systems and services hosted by the Wisconsin Department of Administration (DOA) Department of Enterprise Technology (DET) and cloud hosted services or infrastructure.

This position serves as the principal security technical advisor to the ETF CISO and will serve as the team lead to ensure that ETF successfully manages information security risk. This position serves as the lead in technical initiatives, selection and implementation of tools and processes designed to successfully detect, validate, contain, and remediate cyber threats. To that end, the incumbent provides technical expertise and support in development and implementation of security controls designed to develop a defensive cyber security posture. Additionally, 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 professional, collaborative relationships with internal ETF project teams, DET business and infrastructure teams and ETF contractors and vendors. The incumbent provides technical expertise necessary for the development of information security policy, standards, procedures, and guidelines, and sets an example for ETF staff in following applicable state statute, ETF 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.

## GOALS & WORKER ACTIVITIES

40% GOAL A: Provision of Project Management, Technical Expertise, and Leadership for Security-related Projects

- A1. Lead technical design projects to develop and implement information security controls that protect ETF data across all platforms.
- A2. Function as security technical expert and provide technical direction and operational leadership to cross-functional project teams assigned to deliver security-related solutions, products, and services.
- A3. Lead and advise junior team members installation, configuration, monitoring, validation, and remediation of cyber incidents.
- A4. Oversee projects to research, select, plan for, install, configure, operationalize and maintain technical information security controls for ETF's enterprise-wide business solution application software, including development of processes to address security patches and bug fixes of that software.
- A5. Oversee completion of tasks to ensure timely, accurate and quality project delivery. Provide status and completion reports to CISO.

A6. Work with the CISO to develop information security-related strategic, tactical, and operational plans.

A7. Work with service providers to oversee the secure installation, configuration, operation and maintenance of ETF infrastructure and services.

A8. Represent ETF IS interests and/or act as representative of CISO at state committees, meetings, conferences, or other forums, as directed.

35% GOAL B: Provision of Technical Expertise & Leadership Related to Advanced-level Information Security Support

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

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

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

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

B5. Work with the CISO to develop, implement and periodically test ETF's Incident Response Plan.

B6. Coordinate, lead, and direct BISM and other personnel, as assigned, 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 stakeholders' incident response teams, as appropriate.

B7. 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).

B8. Work with the CISO to plan, budget and operationalize information security-related continuous monitoring of ETF's enterprise.

B9. Provide metrics and other output from information security-related systems and processes to CISO and ETF leadership as requested.

B10. Coordinate maintenance of change management documentation for information security-related systems.

B11. Provide domain administrator support to BITS, when needed.

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

C1. Collaborate with Bureau of Information Technology Services (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 implement standards, procedures, training, and technology that supports ETF's information security strategy.

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

C4. Collaborate with the ETF Office of Communications to ensure quality information security-related messaging to the ETF user community and other relevant stakeholders.

10% GOAL D: Participation in Employment Development Activities

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

D2. Read books and periodicals to improve knowledge of information security and system design principles.

D3. Attend training sessions and workshops to increase knowledge of information security.

D4. Read security reports published by various public and private organizations, to stay current on newly discovered computer security vulnerabilities.

D5. 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.

**KNOWLEDGE, SKILLS, and ABILITIES**

**KNOWLEDGE OF:**

1. Planning, selection, implementation, operations, and maintenance of security-related systems across multiple platforms and applications software.
2. Security related software and configurations specific to Windows desktop and server operating systems.
3. Security-related software and configurations specific to end points and network hardware and software.
4. Security-related technology standards (i.e.- NIST, SANS, CIS, OWASP, ISO, etc.) and their application to enterprise environments.
5. Security-related software and configurations specific to software products, such as Microsoft Office and Microsoft Active Directory.
6. Computer systems and programs unique to the Department of Employee Trust Funds.
7. Security-related Linux distributions and their system and network penetration toolsets.
8. Leadership techniques.
9. Department's purpose, objectives, and mission.
10. Department's technical and business area programs, processes, and requirements.
11. Social engineering techniques and methods.

**SKILLED IN:**

12. Information system (IS) security-related planning, selection, implementation, and documentation processes and best practices.
13. Security-related Linux distributions (i.e. Kali, BlackBox, etc.) and their various system and network penetration toolsets.
14. Operating system and productivity software configuration hardening frameworks such as NIST, SANS, CIS, OWASP, ISO, or similar.
15. IS Security-related planning, selection, implementation, configuration, operations, problem resolution, and maintenance specific to automated software distribution and patching systems, Cisco switches, routers, and firewalls.
16. Adult IS training methods and techniques.
17. Interpersonal communication and communication of technical information effectively in plain language, either orally or in writing to various levels of stakeholders.
18. Use of information technology operations systems.
19. Analyzing system problems and developing solutions.
20. Working independently or as part of a team.
21. Providing consistent quality customer service.
22. Collaborating with a variety of persons at technical, consultant and manager levels.
23. Coordinating, directing, and leading the work of IT professionals or project teams.
24. Providing expertise and problem resolution across multiple platforms and software.
25. Prioritization, organization, and time management.
26. Adapting and adjusting to changes in technology, processes, and priorities.
27. Using the following security tools: vulnerability scanning tools such as Qualys, Nessus, etc.; SIEM tools such as QRadar, Splunk, SolarWinds LEM, etc.; anti-malware tools such as Symantec, Norton, McAfee, etc.; and web filter tools such as ZScaler, Forcepoint, Bluecoat, etc.

**ABILITY TO:**

28. Lead teams assigned the installation, configuring and testing of endpoint hardware, software, network and security software and standards.

29. Lead teams assigned the installation, configuration, and testing of networked peripheral hardware including printers, scanners, etc.
30. Coordinate and lead teams in planning and implementation of network configuration changes, including testing and roll-back planning.
31. Lead teams engaged in security-related planning, selection, implementation, operations, and maintenance of security systems.
32. Lead BISM teams involved in planning, selection, implementation, configuration, operations and maintenance for automated software distribution and patching systems, Cisco switches, routers, and firewalls.
33. Take initiative to assertively represent business needs, to stand firm when necessary and to compromise when possible, to diplomatically challenge assumptions, and to make recommendations to business and technical staff at all levels of responsibility and authority throughout the department.