POSITION # 339114
IS Technical Services Specialist (Identity & Access Management Analyst)
DMS/BITS/ITSCS

POSITION SUMMARY:

Under the general review of the IT Solution Center (ITSC) Supervisor, this position is responsible for providing technical support and assistance for ETF's user access security to systems and applications. This position will guide the user access security environment consisting of Active Directory (AD), 3rd party AD tools, Mainframe Resource Access Control Facility (RACF), STAR/STARFIN systems, legacy application access, and technical Directory and Authentication Services of employees, members, and vendors with the capability to support cloud and on-premise application services. The position will also lead the support of user access security to maintain a secure and healthy user access environment for ETF. The position will work with the Department of Enterprise Technology (DET) as our vendor for technology systems and services.

Major responsibilities include maintenance and support of the mainframe and directory service environments, development and implementation of technical policies and standards for ETF's user authenticated environments and mainframe systems, interaction with agency business managers and IT technical staff to ensure proper security practices are being established and followed, resolution and management of user access problems reported to the ETF Help Desk, and providing technical operations support and backup services as necessary.

This position administers authentication and authorization technologies in use at ETF. This includes working with IT staff, vendors, and partners to setup, configure, and troubleshoot systems that perform authentication and authorization related functions. It also includes working with ETF Security staff to align on security standards and procedures for managing authentication and authorization related processes within the organization. The role requires experience managing technologies that provide multi-factor authentication for users to infrastructure-oriented technologies like email, SharePoint, file servers, etc. as well as custom developed and purchased third party applications. This position also manages end-user authorization for systems that can utilize a centralized tool for authorization such as Active Directory.

GOALS AND WORKER ACTIVITIES:

50% GOAL A: Provision of technical support for enterprise Identity infrastructure, including Identity hardware, software, and services

- A1. Work with business users in setting up user accounts and assisting with problems for the agency.
- A2. Manage users on ETF's Office 365 environment: define new users, groups, distribution lists, reset passwords, etc.
- A3. Review RACF Security audit and control reports and ensure that violations are reviewed, investigated, and needed corrective actions are taken.
- A4. Research and recommend ways to produce and then implement useful and meaningful security information for distribution to department management, including ongoing improvements to existing tracking systems and ad hoc reports.
- A5. Track technical developments that may result in new security capabilities or requirements and recommend appropriate changes.
- A6. Maintain an inventory of ETF's computer security policies and procedures.

A7. Monitor compliance with overall security policies.

A8. Consult with high level technical support peers at ETF or other state agencies and/or vendor(s) technical support as needed to investigate and resolve reported problems.

A9. Participate in the fulfillment of agency requests for identity access services as assigned through the service request process.

A10. Actively participate in the development, documentation and implementation of IT management best practices to ensure the quality of services delivered to customers and partners.

35% GOAL B: Administration of Identity and Access Management for enterprise Identity infrastructure, including Identity hardware, software, and services.

B1. Administer and manage mainframe and LAN security: define new users, dataset and resource profiles, reset passwords, WEB security tables, etc.

B2. Develop and implement technical policies and standards for ETF's LAN and Mainframe systems: Mainframe (RACF), Active Directory, and Identity and Access Management systems hosted internally or with DET.

B3. Monitor identity access data and make recommendations to better utilize resources for optimal performance and cost-effectiveness.

B4. Maintain metrics to measure and evaluate shared IT infrastructure systems and usage.

B5. Maintain awareness of Enterprise policies and procedures to ensure that ETF is compliant with DET standards.

B6. Provide oversight of vendors providing server hardware and software management and other infrastructure services to ensure procedures are being followed and program goals are achieved.

B7. Provide direction for use of procedures along with developing, establishing, and documenting procedures for the proper use and support of enterprise identity access hardware and software.

15% GOAL C: Participate as needed on ETF enterprise projects and special projects assigned by the ITSC Supervisor.

C1. Research and evaluate new tools and technologies and make recommendations on potential benefits for IT and/or business user staff.

C2. Understand and follow published IT management policies and best practices in such areas as Infrastructure Services and Service Support.

C3. Work with security to develop and implement sound security practices and policies that balance the need for security and accessibility of business applications.

C4. Read and discuss pertinent materials to maintain awareness of the operating procedures and environment of BITS.

C5. Participate in ongoing learning opportunities to improve knowledge in responsibility areas.

C6. Complete all other duties and assignments as directed by ITSC Supervisor and CIO.

KNOWLEDGE, SKILLS, AND ABILITIES:

1. Knowledge on concepts of authentication, authorization, active directory policies, active directory federation services (ADFS), and web filtering solutions.
2. Knowledge and skill to provide security administration in a mainframe environment.
3. Knowledge in mainframe automation programing languages such as Resource Access Control Facility (RACF) and Identity and Access Management systems, such as Cayosoft.
4. Knowledge of access role development and maintenance and defining application level roles/groups and permissions to ensure secure authentication and authorization mechanisms are aligned with policies, standards, and best practices.
5. Knowledge of agency audit and compliance requirements.
6. Knowledge of user administration, Active Directory and the user administration functions of a wide variety of multi-user services applications.
7. Knowledge of managing, maintaining, and installing Identity Access and Directory security, account administration and end-point access management, which includes management of service accounts, permissions, passwords, delegation, configuration and the removal of stale accounts
8. Knowledge to support multifactor (MFA) solutions such as RSA, DUO, Microsoft MFA and other identity solutions surrounding multiple methods for user identification.
9. Knowledge of identity security management concepts and software such as different monitoring tools
10. Skill in principles and practices of effective customer relations and oral communication.
11. Ability to work in a team-oriented environment.
12. Strong interpersonal skills to effectively manage business relationships with internal and external customers and business partners.
13. Effective time management skills.
14. Strong written and verbal communication skills.
15. Strong customer service skills and knowledge of best practices.
16. Knowledge and skill in technical problem analysis and resolution.
17. Possess high level of attention to detail and knowledge around quality assurance practices.
18. Ability to multi-task, to be self-initiated, and work independently.