CF OPERATING PROCEDURE
NO. 50-30

STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, June 21, 2023

Systems Management
IDENTITY AND ACCESS MANAGEMENT PLAN

TABLE OF CONTENTS

Page

1. Purpose....3
2. Scope....3
3. Authority....3
4. Policy Statement....3
5. Organizational Security....3
6. Definitions....4
7. Guiding Principles....6
8. Identity and Access Management Governance....6
   8.1. Roles and Responsibilities....6
9. Separation of Duties....8

Separation of Duties is a fundamental principle in the organization's Identity and Access Management (IAM) processes. It ensures that no single individual has excessive control or authority over critical activities, reducing the risk of fraud, errors, and unauthorized access....8

   9.1. User Provisioning and Approval....8
   9.2. Access Review and Certification....8
   9.3. System Administration and Security Administration....8
   9.4. Password Management....8
   9.5. Audit and Monitoring....8
   9.6. Change Management and Release Management....8
   9.7. Incident Response and Remediation....8
10. Identity & Access Management Compliance....8
   10.1. Multi-factor Authentication (MFA)....9
   10.2. Single Sign-On (SSO)....9
   10.3. Continuous Monitoring....9
11. Identification Procedures for Employees and Contractors....9
12. Access Provisioning Procedures for Employees and Contractors....9

12.1. Procedures for a New Employee / Contractor. 9
12.2. Procedures for a Reassigned Employee / Contractor. 10
13. Management Procedures for Employees and Contractors. 11
13.1.Training Programs 12
13.2. Onboarding Process 12
13.3. Ongoing Awareness Campaigns 13
13.4. Role-Specific Training 13
13.5. Security Awareness Resources 13
13.6. Phishing Simulations 13
13.7. Reporting Channels 13
13.8. Policy Acknowledgement 13

1. Purpose. This operating procedure establishes an Identity and Access Management () Plan for the Department of Children and Families (Department) applications in compliance with Rule 60GG-2, Florida Administrative Code (FAC).

2. Scope. This operating procedure applies to anyone who has access to information and data using Department-owned information technology resources including all information technology resources used to support or implement the mission of this Department and any other automated data processing systems in our custody whether owned, purchased, contracted from or to, or leased by the Department. This operating procedure also applies to any information technology resources connecting to the Department's network whether used in offices, in the field, or at telecommuting sites.

3. Authority.

a. Rule Chapter 60GG-2, Florida Administrative Code (FAC), *Florida Cybersecurity Standards*.

b. Department of Children and Families Operation Procedure 50-2, *Security of Data and Information Technology Resources.*

c. Section 282.318, Florida Statutes, *State Cybersecurity Act*.

d. 45 CFR Parts 160 and 164, Subparts A and C, Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules.

e. The Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2 Requirements.

f. 5 U.S.C. 552a, *Privacy Act of 1974 - Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration* (SSA).

g. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5, "*Security and Privacy Controls for Information Systems and Organizations*."

h. Internal Revenue Services (IRS), Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, (11-2021).

4. Policy Statement. This policy establishes the cybersecurity standards per applicable federal and State laws, Executive Orders, directives, regulations, policies, standards, and guidelines. The Department shall hold system users accountable for adhering to policies and procedures which protect confidential data/information from unauthorized modification, destruction, use, or disclosure, including but not limited to Federal Tax Information (FTI). Access to Department resources is granted on the principle of least privilege and enforces the separation of duties so that no individual controls the entire process. Every 365 days or when a significant process change occurs, whichever occurs first, this policy and the resultant procedures should be reviewed and revised.

5. Organizational Security.

a. CIO. Oversight, guidance, final review, and approval.

b. Deputy CIO. Oversight of Enterprise Infrastructure Resources.

c. ISM. Oversight, review, and compliance.

d. Information Security Operations & Administration Team. Oversight of all OITS Identity and Access Management Procedures for Employees, Contractors, and Community Care Based (CBC) organizations.

e. Hiring Manager. Responsible for approving employee and contractor requests for accessing any information system.

f. Human Resources Liaison. Facilitates and assists with Human Resource related activities (e.g., new hires, reassignment, and separation) and provides staff rosters for the physical access review process.

g. OITS Directors & Managers. Responsible for end-dating users in the Information Systems that the OITS Directors and Managers oversee.

h. Program Area. Responsible for ensuring all employees and contractors are in compliance with this operating procedure.

6. Definitions. Terms used in this operating procedure are defined below.

a. Access Management. The IT Security Management process is responsible for allowing users access to and use of IT services, data, or other assets. Access management helps protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. Access management implements information security management policies (also referred to as rights management or identity management).

b. Account Provisioning. The process of granting permissions by creating or changing user accounts or privileges as necessary includes disabling and deleting accounts.

c. Azure Active Directory (AD). A cloud-based identity and access management service developed by Microsoft. AD creates a unique identifier for each individual employee or contractor through their Microsoft account. The Department uses AD in conjunction with OKTA and SailPoint to facilitate the IAM process.

d. Continuous Monitoring. Technology that provides real-time or near-real-time feedback from information systems to enable rapid detection of compliance issues and security risks within IT infrastructure.

e. Contracted Staff. Any person that has been employed to perform a contracted function for the Department through a third party or as an independent contractor.

f. Cybersecurity. The protection afforded to an automated Information System to attain the applicable objectives of preserving the confidentiality, integrity, and availability of Data, information, and information Technology resources.

g. Data. A subset of structured information in a format that allows such information to be electronically retrieved and transmitted.

h. Delegated Access. The cybersecurity principle that requires, when an individual who does not normally have access to a secure system requires access, they will either be given temporary access with a clear start and end date, or they will gain access through an intermediary who has access to the system or data.

i. Employee. Any person employed by the Department in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personal Services (OPS) funds. Also, for the purposes of this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to Department IT resources, including contracted staff and contracted vendor staff.

j. Hiring Manager. The director, manager and/ or supervisor engaged in hiring a new employee.

k. Information Security Manager. The Information Security Manager (ISM) is the person designated by the Secretary of the Department to administer the Department's information technology security program and serve as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards and in accordance with §282.318, Florida Statutes, and Chapter 60GG-2, F.A.C.

l. Information System. Any information resources organized for the collection, processing, creation, maintenance, use, sharing, dissemination, or disposition of digital information.

m. Information Technology Resources (Technology Assets). Equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, disseminate information of any kind or form.

n. Multi-Factor Authentication (MFA). A method of authentication that requires two or more forms of identification (authentication factors) from a user. The three authentication factors are something you know, something you have, and something you are.

o. Office of Information Technology Services (OITS). Department of Children and Families Office of Information Technology Services.

p. Okta. The Department’s Access Management Tool. Okta ensures secure log-in to all applications for all Department employees and contractors.

q. Principle of Least Privilege. The requirement that each business system process, a user, or program must be able to access only the information and resources that are necessary for its business legitimate purpose.

r. SailPoint. An Identity and Access Governance tool used to automate the provisioning into authentication repositories (Active Directory, RACF/Mainframe, LDAP, or related repositories.

s. Separation of Duties. The principle that no user should be given enough privileges to misuse the system on their own, and the process that involves dividing critical tasks and responsibilities among different individuals to create a system of checks and balances. No single individual should have complete control or authority over a process from start to finish.

t. Single-Sign On (SSO). An authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

u. System Owner(s). The entity that owns the data and that has the primary responsibility for decisions relating to a particular data processing system's specifications and usage.

v. System Users. Any person who, through State employment, contractual arrangement, charitable service or any other service arrangement, and with appropriate approvals, would have access to DCF facilities, the Department's information technology resources, or the Department's data for the purpose of conducting business or providing services.

7. Guiding Principles. The department is committed to establishing a comprehensive operational framework, including standards and deliverables, which maximize the confidentiality, integrity, and availability of information technology (IT) resources. To support the Department in continuously meeting this goal, all Department-owned systems fall under the authority of the comprehensive Identity and Access Management policy and shall adhere to the Florida Cybersecurity Standards operating procedure, per Rule 60GG-2. The Department recognizes three steps in this process: Identification of Users, Access Provisioning, and Management of Provisioning.

8. Identity and Access Management Governance

a. Governance Framework: The Department of Children and Families (Department) establishes a Governance Framework to ensure effective management and oversight of the Identity and Access Management Plan. The Governance Framework outlines the roles, responsibilities, policies, and processes related to within the Department.

b. Steering Committee: The Steering Committee is responsible for providing strategic guidance and oversight of initiatives. The committee is composed of key stakeholders, including representatives from the Office of Information Technology Services (OITS), program areas, human resources, legal, and audit. The committee meets regularly to review policies, assess risks, and make decisions regarding implementations and enhancements.

c. Policy Review and Approval: The Policy is subject to regular review and approval by the Steering Committee. The committee ensures that the policy aligns with applicable laws, regulations, and industry best practices. Any updates or revisions to the Policy are documented and communicated to relevant stakeholders.

8.1. Roles and Responsibilities: The Governance Framework defines the roles and responsibilities of individuals involved in processes. These roles include but are not limited to:

a. Chief Information Officer (CIO): The CIO provides oversight and guidance for initiatives and ensures their alignment with the Department's overall IT strategy and goals.

b. Deputy CIO: The Deputy CIO assists the CIO in providing oversight on security policies and initiatives.

c. Information Security Manager (ISM): ISM serves as the process owner for activities and is responsible for developing and implementing policies, procedures, and controls. The ISM works closely with other stakeholders to ensure compliance and effectiveness.

d. Identity and Access Management Administrator: The Administrator is responsible for the day-to-day administration of systems and processes. This includes user provisioning, access requests, access reviews, and user lifecycle management.

e. System Owners: System Owners have the primary responsibility for making decisions regarding access to their respective systems. They work with the Administrator to define access requirements and ensure that access is granted based on the principle of the least privilege.

f. Program Area Representatives: Program area representatives are responsible for ensuring that employees and contractors within their respective areas comply with policies and procedures. They collaborate with the Administrator to address access-related issues and provide necessary approvals for access requests.

d. Auditing and Compliance: Regular audits of processes and controls are conducted to assess compliance with policies and identify areas for improvement. The audit findings are reported to the Steering Committee and appropriate actions are taken to address any identified deficiencies or vulnerabilities.

e. Training and Awareness: The Department provides training and awareness programs to educate employees and contractors about policies, procedures, and best practices. This includes security awareness training, which is mandatory for all system users upon initial access provisioning and on an annual basis thereafter.

f. Performance Monitoring: The Department monitors the performance of processes and systems to ensure their effectiveness and efficiency. Key performance indicators (KPIs) are defined and tracked to measure the success of implementations and identify areas for optimization.

g. Incident Response: The Department has established an incident response process to address -related incidents, such as unauthorized access attempts or data breaches. The process includes incident detection, containment, eradication, and recovery, as well as post-incident analysis and remediation.

h. Program Review: The Governance Framework includes regular program reviews to evaluate the overall effectiveness of initiatives and identify opportunities for improvement. The program reviews assess the alignment of business objectives, the adequacy of controls, and the compliance with applicable laws and regulations.

i. Documentation and Records Management: The Department maintains comprehensive documentation and records related to processes, policies, procedures, and controls. These records include access requests, access reviews, user provisioning and deprovisioning activities, and audit reports. The documentation is regularly updated and securely stored for reference.

9. Separation of Duties
Separation of Duties is a fundamental principle in the organization's Identity and Access Management (IAM) processes. It ensures that no single individual has excessive control or authority over critical activities, reducing the risk of fraud, errors, and unauthorized access.

9.1. User Provisioning and Approval: The process of granting access to systems and resources is divided into multiple steps involving different individuals or roles. For example, the request for access is submitted by the user's manager or supervisor, while the approval is performed by a separate designated approver or an access control board. This separation ensures that access requests are independently reviewed and approved, minimizing the potential for unauthorized access.

9.2. Access Review and Certification: Regular access reviews are conducted to validate the appropriateness of user access rights. These reviews involve individuals or roles separate from those responsible for user provisioning. For instance, a manager or supervisor performs access reviews for their team members, ensuring that access privileges align with the users' job responsibilities. This separation helps identify and mitigate any access-related risks or violations.

9.3. System Administration and Security Administration: The roles of system administrators and security administrators are distinct and segregated to enforce separation of duties. System administrators have administrative privileges to manage and maintain system functionality, while security administrators oversee access controls, user roles, and security policies. This separation prevents conflicts of interest and unauthorized modifications to access permissions.

9.4. Password Management: The organization employs a password management process that separates the responsibilities of password creation, resetting, and recovery. For instance, users may be responsible for creating their passwords, while helpdesk personnel or a dedicated password administrator assists with password resets. This segregation prevents abuse of privileges and unauthorized access due to compromised passwords.

9.5. Audit and Monitoring: The responsibility for auditing and monitoring IAM processes is separate from the operational roles involved in access provisioning and management. Independent auditors or a dedicated internal audit team perform periodic reviews of access controls, user activity logs, and system configurations to detect anomalies, identify compliance gaps, and ensure adherence to IAM policies. This separation adds an additional layer of oversight and reduces the risk of fraudulent activities going unnoticed.

9.6. Change Management and Release Management: The organization follows separate change management and release management processes, each with its own set of responsibilities and controls. Change management focuses on assessing, approving, and implementing changes to the IAM system, while release management deals with the deployment and rollout of system updates and enhancements. This separation minimizes the risk of unauthorized or untested changes impacting system integrity.

9.7. Incident Response and Remediation: The incident response process includes separate roles for incident detection, analysis, containment, and remediation. These roles are carried out by different individuals or teams to prevent a single person from having complete control over incident handling. For example, security analysts may be responsible for incident detection and analysis, while IT administrators handle system remediation. This segregation ensures a comprehensive and impartial response to security incidents.

10. Identity & Access Management Compliance. All Identity & Access Management applications and systems used by the Department shall adhere to the following requirements:

10.1. Multi-factor Authentication (MFA): The application must require two or more forms of identification (i.e., something you know, something you have, something you are) from the user when creating their unique Identity used to provision account access and whenever the user attempts to access their provisioned accounts.

10.2. Single Sign-On (SSO): All applications access via provisioning through the IAM Plan must be accessed via a single sign-on account, the activity of which can be monitored, reviewed, and audited by the department.

10.3. Continuous Monitoring: All department applications should allow the department to monitor user activity and access logs for review and audit. The data provided by these logs should be sufficient to analyze access patterns to identify anomalies and potential security risks to the department and its systems.

11. Identification Procedures for Employees and Contractors.

a. Per CFOP 50-02, prior to using the Department's information technology resources, system users will sign form CF 114, "Security Agreement Form" (available in DCF Forms), to acknowledge receipt of and confirm agreement to abide by the minimum DCF security requirements specified therein.

b. Department employee supervisors will sign and forward the original copy of CF 114 to the Office of Human Resources and the Office of Human Resources will place the original in the employee's personnel folder. Employees will retain a copy of CF 114 and attachments.

c. After system users have signed form CF 114 and completed and signed their DCF Access Authorization Form, those documents will be attached to an IT Statewide Help Desk request for assignment of a unique personal identifier (User ID and Password) to each person who uses information technology resources to access the Department data processing systems and Department data by means of information technology resources owned, purchased, or leased by the Department. It is the policy of this Department that system users shall complete Security Awareness Training within 24 hours of being assigned a personal identifier and within the first 10 days of employment by the Department.

d. In addition, DCF employees must sign form CF 114, "Security Agreement Form," within ten days of employment and annually to acknowledge receipt of and confirm agreement to abide by 'the minimum DCF security requirements specified therein.

e. The identifier(s) will permit access to the data that the person has a need and right to know and will control inquiry and update capabilities. The system owner will determine and authorize system access according to the principles of least privilege and delegated access, with no access given that is not absolutely necessary for business needs.

12. Access Provisioning Procedures for Employees and Contractors.

12.1. Procedures for a New Employee / Contractor.

a. When any employee or contractor needs access to an information system, the employee or contractor must complete form CF 0138 (the physical version) and request access to the associated

system by inputting a ticket into the DCF IT Statewide Help Desk ticketing process. Otherwise, the employee or contractor must complete the AAR form (the digital version), which will automatically input a ticket into the DCF IT Statewide Help Desk ticketing process. Wherever CF 0138 is mentioned in this process, the AAR form will represent a functional alternative, unless otherwise noted.

(1). The Hiring Manager (or designee) ensures that the employee completed the required DCF Security Awareness Training and CF 0114, the DCF Security Agreement Form. It is necessary to receive access to sensitive Department data after an employee acknowledges the associated responsibilities of being granted access to such data.

(2). The Human Resource Liaison obtains proof that the new hire received the required Security Awareness Training in the form of a certificate or e-acknowledgement and proof of completion of CF 0114, the DCF Security Agreement Form, in the form of a hand-signed copy or an e-acknowledgement.

b. The Hiring Manager approves the employee or contractor's complete CF 0138 or AAR form via the DCF IT Statewide Help Desk ticketing process.

c. The Human Resources Liaison submits the completed resource access request form(s) and associated proof of requirements being met to the DCF Statewide Help Desk for provisioning by the Security Operations and Administration Team.

d. The Security Operations and Administration Team uses the unique identifiers created during the hiring process to grant the user access to the requested system.

12.2. Procedures for a Reassigned Employee / Contractor.

As per CFOP 50-2, *Security of Data and Information Technology Resources*, supervisors and managers are responsible for ensuring the removal of user access to IT resources of their direct reports once it is no longer appropriate:

a. When an employee moves from a position under one department supervisor to a position under another department supervisor, the new department supervisor is responsible for ensuring the employee has access to IT resources required to perform their new job duties. The new supervisor must complete and submit a new CF 138 through the DCF IT Statewide Help Desk ticketing process.

b. When an employee moves to another position (i.e., a new position number and/or position description) but maintains the same supervisor:

1) The supervisor must review the IT resources the employee has access to and determine which IT resources are required to perform their new job duties.

2) If modification is required:

a) The supervisor must complete and submit a copy of CF 138 via the DCF Statewide Help Desk.

b) Then, provide the Help Desk ticket number and a copy of the CF 138 to the OITS Human Resource Liaison.

3) If no modification of the employee's access is necessary in this same-supervisor scenario, no CF 138 needs to be completed and the supervisor should move forward with the HR processes.

c. The Human Resource Liaison will work with the employee's supervisors to facilitate the successful reassignment of any employee.

d. The previous supervisor of a reassigned employee or contractor must review all work products the reassigned employee created under their supervision to determine what should be retained, moved, or deleted, and then take the appropriate action.

12.3. Procedure for Employee / Contractor Separation.

a. When an employee provides verbal or written notification of their separation date, the supervisor (or designee) must review the IT resources the employee has access to and remove access by submitting a copy of CF 138 to the DCF Statewide Help Desk no later than the employee's last day of work; per CFOP 50-2, Chapter 2. Once the supervisor has received the Help Desk Ticket number, the supervisor must provide that number and a copy of the CF 138 to the Human Resource Liaison.

b. The Human Resource Liaison will work with supervisors to facilitate the separation of a former DCF employee.

c. Upon receipt of the DCF Statewide Help Desk Ticket, OITS Security Operations & Administration team will immediately schedule the disabling of the accounts assigned to the separating employee. When necessary, the appropriate supervisor or the Human Resource Liaison may contact the OITS Security Operations & Administration team directly to request emergency removal of access, then follow up with the standard procedure.

13. Management Procedures for Employees and Contractors.

a. Systems will automatically disable user IDs that have not been used for a period of 30-60, days, depending on risk level. Business systems must force users to change their passwords every 30-90 days, based on the assessed risk of the system. Network system users must change passwords every 90 to 180 days, based on risk, or the user's account will automatically lock. Business and network systems must enforce a minimum password age restriction of one day.

b. Department supervisors and managers are responsible for coordinating with Human Resources and with the OITS Security Operations & Administration team to ensure the removal of the system user's access to an IT resource once it is no longer appropriate by an employee they supervise:

(1) Upon receipt of written or verbal notification of a system user's resignation or separation from the Department, the supervisors and managers are responsible for:

(a) Coordinating with Human Resources to ensure the timely submission of the employee's separation package to the Human Resources Shared Services Center (HRSSC) for review and processing, per CFOP 60-70, Chapter 1.

(b) Using the DCF IT Statewide Help Desk ticketing process to notify the OITS Security Operations & Administration Team to request the removal of previously authorized system access within 24 hours of determining system access is no longer appropriate, including any Administrative Accounts. Upon receiving the DCF IT Statewide Help Desk Ticket, the OITS Security Operations & Administrations Team will disable the system user's access accounts and document the process in the IT Statewide Help Desk Ticket. The description of the access removal process in the IT Statewide Help Desk Ticket should include the name of each IT resource the employee had access to and the date and time of the access removal. When necessary, the Department supervisor and manager may contact the DCF Statewide Help Desk directly to request emergency removal of access, then follow up with the standard procedure.

(2) When a DCF employee changes from one position description to another at the Department, the new supervisor is responsible for ensuring access to IT resources no longer required by that employee to perform their new job duties are removed, and the removal process is documented in an IT Statewide Help Desk Ticket. Supervisors and managers should contact the OITS Security Operations & Administration Team with any questions about the removal of access process for IT resources that are no longer required.

(3) When a DCF Administrative Account is needed for staff to complete regular work duties that require elevated privileges, the supervisor must put in a ticket via the DCF Statewide Help Desk ticketing process. The OITS Active Directory and Messaging Team will review the ticket and create the account. DCF Administrative Accounts are ONLY to be used to launch and run a work required process that requires elevated privileges; no other use is permitted.

c. After the OITS Security Operations & Administration Team removes a user's access to an information system, it is the responsibility of the OITS Directors and Managers whose teams oversee those systems to ensure that all user accounts are end-dated within 120 days of the user's access being removed.

13. User Awareness and Training

Educating users about their responsibilities, best practices, and potential risks associated with access management enhances their understanding of the IAM processes and promotes a culture of security within the organization.

13.1. Training Programs: Conduct regular training programs to educate users on the principles of Identity and Access Management, access management policies, and procedures. These training sessions may cover topics such as password security, access request and approval processes, data handling practices, and user responsibilities. The training programs are tailored to different user groups based on their roles and access requirements.

13.2. Onboarding Process: During the onboarding process, new employees receive specific identity and access management training as part of their orientation. This training familiarizes them with the organization's identity and access management policies, procedures, and user responsibilities.

Additionally, new employees are educated on the importance of secure access practices, the consequences of policy violations, and the procedures for requesting and managing their access rights.

13.3. Ongoing Awareness Campaigns: Conduct regular awareness campaigns to reinforce good practices among all users. These campaigns may include posters, email newsletters, intranet articles, and interactive quizzes to engage users and promote awareness. The topics covered may include password hygiene, phishing awareness, social engineering, and the importance of reporting suspicious activities.

13.4. Role-Specific Training: Different user groups may require role-specific training based on their responsibilities within the identity and access management system. For example, managers and supervisors may receive additional training on access review and certification processes, while system administrators may undergo specialized training on managing user roles and permissions. This targeted training ensures that users have the necessary knowledge and skills to fulfill their identity and access management related responsibilities effectively.

13.5. Security Awareness Resources: Maintain a repository of security awareness resources related to identity and access management.

13.6. Phishing Simulations: To strengthen users' ability to identify and report phishing attacks, conduct periodic phishing simulations. These simulations involve sending simulated phishing emails to users and tracking their responses. The results are used to identify areas for improvement and provide targeted training and awareness on recognizing and reporting phishing attempts.

13.7. Reporting Channels: Establish clear reporting channels for users to report any issues, such as suspicious access requests, unauthorized access, or potential policy violations. These channels can include dedicated email addresses, helpdesk support, or incident reporting systems. Users are encouraged to report any security concerns promptly to facilitate timely investigation and remediation.

13.8. Policy Acknowledgement: Users are required to acknowledge and sign off on identity and access management policies and procedures to signify their understanding and compliance. This ensures that users are aware of their responsibilities and the consequences of non-compliance.

BY DIRECTION OF THE SECRETARY:

(*Signed copy on file*)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL
New operating procedure.