|  |  |  |
| --- | --- | --- |
| Policy #: | Title: | Effective Date: |
| 1 | ACCOUNT MANAGEMENT Policy | 04-09-25 |

PURPOSE  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

REFERENCE  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**NIST SP 800-53, NIST SP 800-53a, NIST SP 800-63, NIST SP 800-161, NIST SP 800-207, NIST SP 800-193, FIPS 200, FIPS 201.**

**ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017(**Acest standard se referă la securitatea informațiilor în cloud computing și include aspecte legate de gestionarea conturilor în medii cloud.**), ISO/IEC 27018, ISO/IEC 27035.**

POLICY  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This policy is applicable to all departments and users of S.R.L `CloudSec` resources and assets.

ACCOUNT MANAGEMENT

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use

within the system;

b. Assign account managers;

c. Require **Autentificare multi-factor (MFA)** for group and role membership;

d. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (i.e., privileges) **and level of access** for each account;

e. Require approvals by **information security officers** for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with **account management procedures**;

g. Monitor the use of accounts;

h. Notify account managers and **Cloud Service Administrators** within:

1. Notify account managers and Cloud Service Administrators within 24 hours when accounts are no longer required.

2. Notify account managers and Cloud Service Administrators within 48 hours when users are terminated or transferred.

3. Notify account managers and Cloud Service Administrators within 72 hours when system usage or need-to-know changes for an individual.

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. **User Role, Department or Team, Project Affiliations, User Experience or Certifications**;

j. **Review accounts for compliance with account management requirements quarterly;**

k. Establish and implement a process for changing shared or group account authenticators (if

deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Discussion: Examples of system account types include individual, shared, group, system, guest,

anonymous, emergency, developer, temporary, and service. Identification of authorized system

users and the specification of access privileges reflect the requirements in other controls in the

security plan. Users requiring administrative privileges on system accounts receive additional

scrutiny by organizational personnel responsible for approving such accounts and privileged

access, including system owner, mission or business owner, senior agency information security

officer, or senior agency official for privacy. Types of accounts that organizations may wish to

prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and

guest accounts.

Where access involves personally identifiable information, security programs collaborate with

the senior agency official for privacy to establish the specific conditions for group and role

membership; specify authorized users, group and role membership, and access authorizations for

each account; and create, adjust, or remove system accounts in accordance with organizational

policies. Policies can include such information as account expiration dates or other factors that

trigger the disabling of accounts. Organizations may choose to define access privileges or other

attributes by account, type of account, or a combination of the two. Examples of other attributes

required for authorizing access include restrictions on time of day, day of week, and point of

origin. In defining other system account attributes, organizations consider system-related

requirements and mission/business requirements. Failure to consider these factors could affect

system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish

temporary accounts as part of normal account activation procedures when there is a need for

short-term accounts without the demand for immediacy in account activation. Organizations

establish emergency accounts in response to crisis situations and with the need for rapid account

activation. Therefore, emergency account activation may bypass normal account authorization

processes. Emergency and temporary accounts are not to be confused with infrequently used

accounts, including local logon accounts used for special tasks or when network resources are

unavailable (may also be known as accounts of last resort). Such accounts remain available and

are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating

accounts include when shared/group, emergency, or temporary accounts are no longer required

and when individuals are transferred or terminated. Changing shared/group authenticators when

members leave the group is intended to ensure that former group members do not retain access

to the shared or group account. Some types of system accounts may require specialized training.

Related Controls:

1. AC-2: Account Management
2. AC-3: Access Enforcement
3. AC-5: Separation of Duties
4. AC-6: Least Privilege
5. AC-17: Remote Access
6. AC-18: Wireless Access
7. AC-20: Use of External Information Systems
8. AC-24: Access Control Decisions
9. AU-2: Audit Events
10. AU-12: Audit Generation
11. CM-5: Access Restrictions for Change
12. IA-2: Identification and Authentication (Organizational Users)
13. IA-4: Identifier Management
14. IA-5: Authenticator Management
15. IA-8: Identification and Authentication User-Displayed Value
16. MA-3: Maintenance Tools
17. MA-5: Maintenance Personnel
18. PE-2: Physical Access Authorizations
19. PL-4: Rules of Behavior
20. PS-2: Publicly Accessible Content
21. PS-4: Personnel Termination
22. PS-5: Personnel Transfer
23. PS-7: Third-Party Personnel Security
24. PT-2: Security Function Isolation
25. PT-3: Security Functionality Verification
26. SC-7: Boundary Protection
27. SC-12: Cryptographic Key Establishment and Management
28. SC-13: Use of Cryptography
29. SC-37: System and Communications Protection

COMPLIANCE

Individuals who violate this policy may face appropriate disciplinary actions, including termination of employment or service contracts, restriction or revocation of access to IT resources, and other suitable measures. Additionally, civil and criminal penalties may be enforced in accordance with applicable laws.

POLICY EXCEPTIONS

Requests for exceptions to this cloud service policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments or teams requesting exceptions shall submit their requests to the CIO. The request should clearly outline the scope of the exception, provide justification for granting the exception, assess the potential impact or risk associated with granting the exception, propose risk mitigation measures to be implemented by the IT Department, and outline initiatives, actions, and a timeframe for achieving compliance with the policies outlined herein. The CIO shall review such requests and consult with the requesting department.