|  |  |  |
| --- | --- | --- |
| Policy #: | Title: | Effective Date: |
| 1 | **Physical Access Control Policy in CloudComP** | 05-14-25 |

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

To ensure that access controls are appropriately implemented and maintained in compliance with IT security policies, standards, and procedures within a cloud computing environment.

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

* **National Institute of Standards and Technology (NIST) Special Publications (SP):**
  + NIST SP 800-53a – Access Control (AC)
  + NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94
  + NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121
  + NIST SP 800-124, NIST SP 800-164
* **NIST Federal Information Processing Standards (FIPS) 199**

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

This policy applies to all departments and users of CloudComP resources and assets within the cloud infrastructure.

**ACCOUNT MANAGEMENT**

**IT Department shall:**

* Identify and select various types of information system accounts (individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service) to support organizational missions and business functions.
* Assign account managers for these accounts.
* Establish conditions for group and role membership.
* Specify authorized users, group and role membership, and access authorizations (privileges) for each account.
* Require system owner approvals for creating information system accounts.
* Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
* Monitor the use of information system accounts.
* Notify account managers of changes in account necessity or user status.
* Authorize access based on valid access authorization.
* Review accounts for compliance with account management requirements at [defined frequency].
* Employ automated mechanisms to support account management.
* Ensure that temporary and emergency accounts are automatically disabled after defined usage or time period.
* Automatically audit and notify IT personnel of account management actions.

**ACCESS ENFORCEMENT**

**IT Department shall:**

* Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

**INFORMATION FLOW ENFORCEMENT**

**IT Department shall:**

* Control the flow of information within the system and between interconnected systems based on approved authorizations.

**SEPARATION OF DUTIES**

**IT Department shall:**

* Separate duties of individuals where necessary to prevent malevolent activity without collusion.
* Document and define access authorizations to support separation of duties.

**LEAST PRIVILEGE**

**IT Department shall:**

* Employ the principle of least privilege for all users.
* Explicitly authorize access to hardware and software controls.
* Ensure privileged functions and security-relevant information are restricted to defined personnel or roles.

**REMOTE ACCESS**

**IT Department shall:**

* Establish and document remote access restrictions and requirements.
* Monitor and control remote access methods.
* Use cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

**WIRELESS ACCESS**

**IT Department shall:**

* Establish and document wireless access restrictions and requirements.
* Protect wireless access through user and device authentication and encryption.

**ACCESS CONTROL FOR MOBILE DEVICES**

**IT Department shall:**

* Establish restrictions and requirements for mobile devices.
* Authorize and monitor connections of mobile devices to the cloud services.
* Employ encryption to protect the confidentiality and integrity of data on approved mobile devices.

**COMPLIANCE**

Employees and non-employees who violate this policy may face disciplinary actions, including termination and civil or criminal penalties.

**POLICY EXCEPTIONS**

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), including a detailed justification and risk mitigation measures.

**RESPONSIBLE DEPARTMENT**

Chief Information Office and Information System Owners