Vera C. Rubin Observatory
Rubin Observatory Project Office

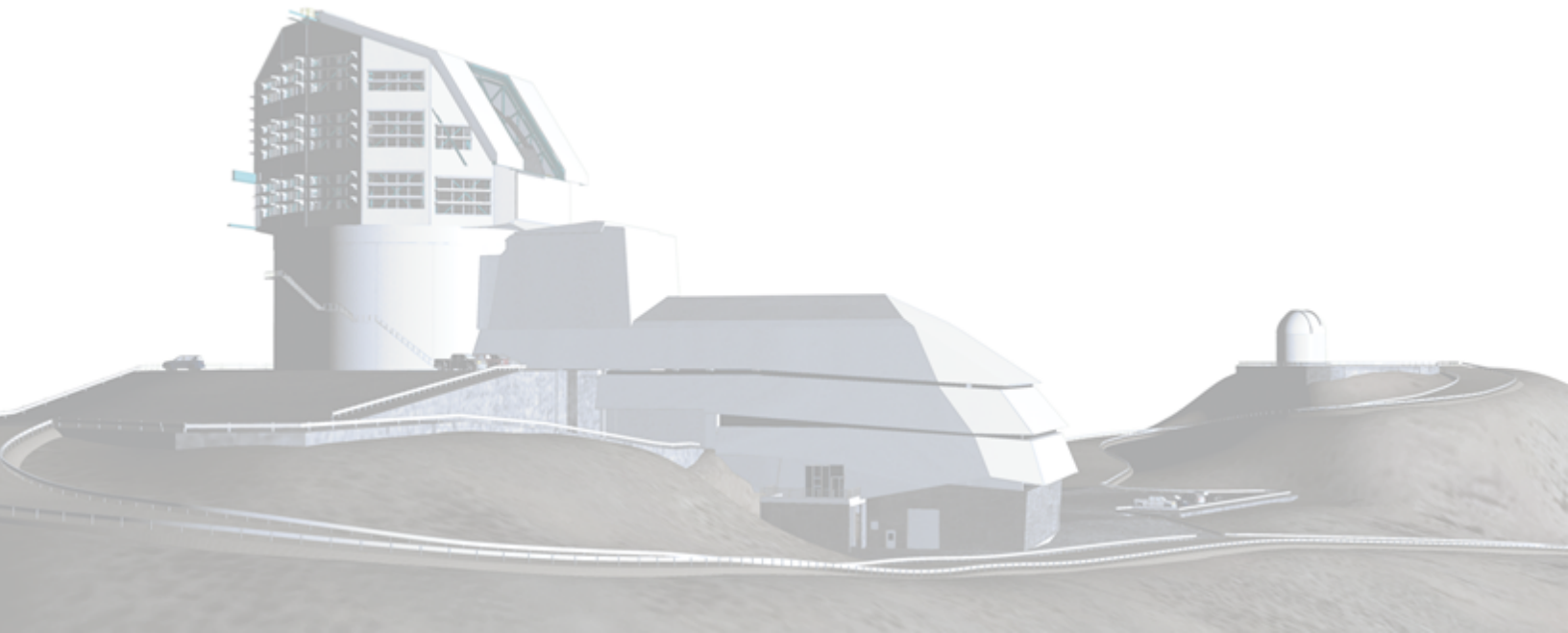
Access Control

Cristian Silva, Joshua Hoblitt

ITTN-068

Latest Revision: 2024-11-08

DRAFT



Abstract

Access control policies

Change Record

Version	Date	Description	Owner name
1	2023-01-20	Unreleased.	Joshua Hoblitt
1	2023-10-03	Unreleased.	Cristian Silva

Document source location: `https://github.com/lsst-it/ittn-068`

Contents

Access Control

1 Introduction

This Access Control Policy defines the principles, procedures, and guidelines for granting, monitoring, and revoking access to information systems, data, and resources at Vera C. Rubin Observatory. It ensures compliance with NIST 800-171 standards, which protect Controlled Unclassified Information (CUI).

2 Policy Statement

2.1. Access Control Framework (AC-2)

- **Justification:** AC-2 requires an access control framework. Our policy follows this requirement by providing a framework rooted in least privilege and need-to-know principles.
- **Fulfillment:** Our access control framework ensures that access rights are assigned based on job roles and responsibilities, adhering to the least privilege principle. This limits users' access to only what is necessary for their duties.

2.1 User Authentication (IA-2)

- **Justification:** IA-2 mandates user authentication. Our policy aligns with this requirement by enforcing multi-factor authentication (MFA) and strong password policies.
- **Fulfillment:** 2FA is required for all users accessing our systems. Strong password policies ensure that user credentials meet security standards.

2.2 Access Channels (SC-7)

- **Justification:** SC-7 requires securing remote access.
- **Fulfillment:** Remote access to our systems is only permitted through secure VPN connections.

2.3 Role-Based Access Control (AC-3)

- **Justification:** AC-3 emphasizes role-based access control (RBAC).
- **Fulfillment:** Access to resources is granted based on job roles and responsibilities, aligning with RBAC principles. Users are assigned roles that define their access permissions.

2.4 Access Request Process (AC-5)

- **Justification:** AC-5 stipulates the need for access requests.
- **Fulfillment:** Access to our systems and resources is obtained through a formal request process.

Access Request Procedures:

a. Employees or authorized personnel request access by opening an IHS ticket specifying the desired access

b. The ticket includes the requester's name, department, job title, specific systems or resources required, the reason for access, and access duration.

c. The IT department reviews and validates access requests, ensuring alignment with job roles, responsibilities, and the principle of least privilege.

d. IT along with the owner of the system approve access and is communicated to the requester via the IHS ticket.

e. Access is regularly reviewed and audited to maintain compliance.

2.5 Access Revocation (AC-7)

- **Justification:** AC-7 mandates immediate access revocation upon personnel changes.
- **Fulfillment:** Access to our systems is immediately revoked upon notification of personnel changes.

Access Revocation Procedures:

a. HR notifies the IT department by using the offboarding form.

b. IT revokes the access based on the need date in the offboarding form.

2.6 Monitoring and Logging (AC-19)

- **Justification:** AC-19 requires monitoring and logging.
- **Fulfillment:** IT deploys a Security Information and Event Management (SIEM) system to monitor access and system activities. Logs are reviewed for anomalies and security incidents.

Monitoring and Logging Procedures:

a. The IT department deploys a Security Information and Event Management (SIEM) system to monitor access and system activities.

b. Logs are reviewed [frequency] for anomalies and security incidents.

c. Security incidents and unauthorized access attempts are logged, investigated, and reported promptly.

3 Responsibilities

3.1 Responsibilities (AC-2, AC-5)

- **Justification:** AC-2 and AC-5 emphasize user responsibilities. Our policy mandates employees and users protect their authentication credentials and follow access request procedures.
- **Fulfillment:** Users are responsible for safeguarding authentication credentials, including usernames, passwords, and authentication tokens. They are also required to promptly report any suspicious activities or security incidents to IT

3.1.1 User Responsibilities:

a. Safeguard authentication credentials, including usernames, passwords, and authentication tokens.

b. Promptly report any suspicious activities or security incidents to IT.

c. Communicate to IT if the role based access needs modifications (more or less)

3.1.2 IT Responsibilities:

a. Manage and maintain the access control framework.

b. Conduct regular access reviews and audits.

c. Implement and maintain the system for real-time monitoring.

4 Compliance and Enforcement

4.1 Compliance (AC-1, AC-2)

- **Justification:** AC-1 and AC-2 require policy compliance. Non-compliance may result in disciplinary actions, as outlined in our policy.
- **Fulfillment:** Periodic compliance audits will be conducted . Violations will be reported to upper management.

5 Review and Revision

- **Justification:** NIST 800-171 doesn't specify review and revision explicitly. However, regular policy reviews are essential to align with changing threats and organizational needs. Our policy aligns with this principle.

A References

B Acronyms

Acronym	Description
DM	Data Management