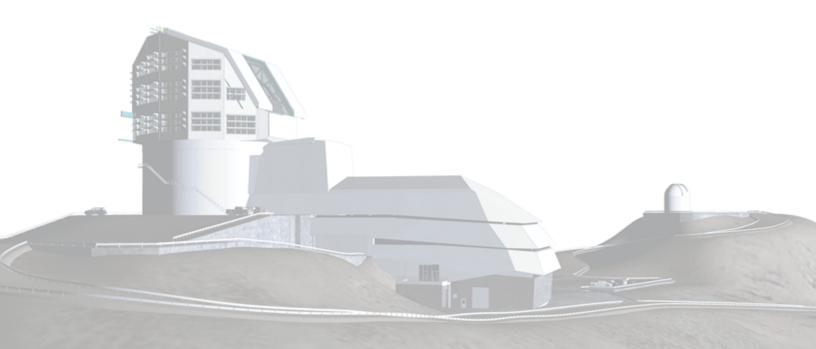# Vera C. Rubin Observatory
Rubin Observatory Project Office

Access Control

Joshua Hoblitt

ITTN-068

Latest Revision:

Abstract

Access control policies

Change Record

Version	Date	Description	Owner name
1	YYYY-MM-DD	Unreleased.	Joshua Hoblitt

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

Contents

Access Control

> Anybody who has an identity problem had better wise up and get with the program!
>
> *Jack Handey*

1 Introduction

applies primarily to information technology related infrastructure for both electronic and physical access.

Conforms to NIST 800-53

The concept of "Least Privilege" is employed per 800-53r5 3.1 AC-6.

LEAST PRIVILEGE

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#%5B%7B%22num%22%3A181%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C88%2C336%2C0%5D

Resouce Owners

All resources should have one or more "owners" for the proposes of access control. In order for a user to be granted access to a resource an owner will need to sign-off on that request. resource owners are also responsible for auditing the list of authorized users for resource and filing requests to remove access when a user no longer requires use of the resource

General workflow

- open an IHS ticket and request access to X resource - A resource owner must sign off on the ticket before access may be granted

A References

B Acronyms

Acronym	Description
DM	Data Management