	NOIRLab	Pages: 15

NOIRLab Workplace Security Plan

26 April 2021

Author List:

C. Gessner / Head of Safety, Health, and Environment	

Contents

Distribution List

External Distribution

Institution / Body/ Committee	Copy
ABOD	
NMOC	
NSF	

Internal Distribution

Name	Copy

Change Record

Version	Date	Description	Owner(s) Name(s)
Final	6.7	Final version	C. Gessner
Final	6.7	Edited and formatted in template	S. Hunt
Final	4.6	Changed NCOA to NOIRLab	S. Hunt

Reference Documents

Document Name	Document Reference	Location

Approval Signature Record

Reviewer Role	Title	Name/Signature
Document Author		
Reviewer 1		
Reviewer 2		

Reviewer Role	Title	Name/Signature
Reviewer 3		
Document Administrator		
Approved by		
Accepted by		

Purpose

This document provides a description of the NSF's National-Optical Infrared Astronomy Resaerch Laboratory (NOIRLab) Workplace Security Plan. The Plan focuses on personnel and equipment workplace security for all NOIRLab operations (sites) and projects. This plan is a basis of compliance for all NOIRLab sites.

Introduction

The management of NOIRLab is dedicated to the protection of its employees, visitors, information, facilities, and other assets from any security threat affecting our company to eliminate or reduce the probability of injury or loss. Management places a high priority on developing, validating, and, if necessary, implementing our company's Workplace Security Plan. This plan is a basis of compliance for all NOIRLab sites.

Objective

This Plan establishes and defines security procedures and requirements for NOIRLab consistent with all U.S. and Chilean laws and regulations. The objective of the plan is to make security management an integral part of operations and construction activities.

Management, technical support staff, system administrators, safety staff, and security personnel are responsible for facility access requirements. The management and monitoring of physical access to facilities is important and help improve employee security and safety and reduces loss. All employees are encouraged to make security and safety a personal initiative.

If after reading this plan, you find that improvements can be made, please contact the Head of Safety, Health, and Environment.

Integrated with Other Plans and Policies

This plan is integrated with the Safety, Health and Environment Plan (link here) and Emergency Plan (link here). NOIRLab also has an IT Cybersecurity Plan (link here). Parts of other plans, such as emergency evacuation plan, can be used in planning how to respond to a criminal activity or violent emergency. Annual training should include information on all plans.

Workplace Security

Workplace security is the ability to control physical access to the workplace and to control specific locations inside the workplace. This includes controlling unauthorized access during non-business hours and denying access to unauthorized or dangerous persons when employees are present. Methods to enhance workplace security is an attempt to minimize crime.

Security Risks

Security risks related to this plan are

- intrusion
- vandalism
- theft
- acts of violence
- acts of terrorism

Security Guard Services

Sites should consider security guard services based on local crime rates and experience. Some sites contract with third party security guard services. Tucson utilizes nighttime guard services, the La Serena *recinto* provides full-time guard services, and the AURA Observatory property is provided with guard services at the *control puerta*.

Security Cameras

Sites should consider deploying security cameras in areas where enhanced security and safety is needed. Placement of security cameras may be based on past experience. Security cameras are usually monitored by Facilities and/or IT. A security camera may provide response to an event and provides a record of an event for regulatory authorities. Security cameras are not appropriate for monitoring employee productivity.

Lighting

Where practical at office locations, exterior lighting that complies with local ordinances and laws might be used to provide lighting at entrances of office locations.

Exterior Doors

Exterior doors on buildings should be substantial enough to deny quick entry by force. Consideration should be made as to whether all exterior doors should be locked by a key or keycard. Exterior doors shall have panic bars or devices that allow a person to exit easily in an emergency. Site Facilities shall be immediately notified if lock hardware becomes loose or door-closing devices or latches are not working correctly. Unknown or suspicious person(s) shall not be allowed to gain access by following employees through a locked door. Employees should take action by asking if the person has a key card or if they are visiting someone. Employees should notify site Facilities if the person is suspect. Exterior doors should not be propped open without supervision.

Windows

Windows should not open far enough for a person to enter or reach through to open a latch.

Locks and Keys

Most office locations are equipped with either electronic key card access systems and/or hard keys. Each Site facility shall assigned access coordinator(s). The access coordinator(s) role is an important method of key control to support the physical security of the buildings. A method of accounting of all keys shall be in place for key cards and hard keys. Spare keys shall be controlled and secured. If keys are lost or damaged, immediately report to the local Facilities office. Keys and key cards should not be shared or loaned to others.

The process for granting card and/or key access resides with the site Facilities. They shall regularly review card and/or key access rights and remove access for individuals that no longer require access or persons who leave the company. Access rights shall be based on an employee's (staff, visitor, contractor, etc.) role or function in the organization. Key card data is not appropriate for monitoring employee productivity.

Interior Doors

To reduce the temptation of theft, office doors should be locked after hours or when not attended. Site facilities managers should lock doors to computer rooms, HVAC rooms, laboratories, phone system rooms, mailrooms, vacant rooms, laboratories, and maintenance areas. As a refuge from a dangerous person, there should be enough rooms for employees to shelter in place during an emergency.

Restricted-Access Areas

Consideration should be made to designate offices and areas of the workplace that have restricted access such as locations where there is the personnel information, Human Resources offices, Senior Management offices, financial and contracts offices, mail-sorting areas, laboratories, and other areas that have high value items. Consideration should be made to protect restricted access areas by key card entry control. Other methods of control may include the following.

- All areas containing sensitive information shall be physically restricted.
- All individuals in these areas must have a keycard on their person if a manager requests to see it.
- Restricted IT areas such as data centers, computer rooms, telephone closets, a network router, hub rooms, voicemail system rooms, and similar areas containing IT resources shall be restricted based upon functional business needs.

- Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted.
- Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information.
- Appropriate facility entry controls shall limit and monitor physical access to information systems.
- Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas, and this data shall be stored for at least three months, unless otherwise restricted by rule, regulation, statute, or law.
- Physical access to all restricted areas shall be documented and managed. All restricted areas must be physically protected relative to the criticality or importance of the function or purpose of the area managed.
- Requests for access shall come from the applicable manager in the area where the data/system resides. Access to restricted area will be granted only to personnel whose job responsibilities require access. Electronic access control systems shall be used to manage access to controlled spaces and facilities.

Firearms

Firearms are prohibited on the sites, except when political dignitaries are protected by armed security or law enforcement visits.

Law Enforcement – Department Having Jurisdiction

If a crime either is in progress or is suspected, local law enforcement shall be notified as the first responders. Dialing 911 at sites within the U.S. and dialing 133 in Chile will prompt the first responders. Because all sites are either owned or partially owned by the U.S. federal government, the U.S. FBI nearest field office should be contacted. Arizona FBI field office 623-466-1999. Hawai'i FBI field office 808-566-4300.

Contractors, Visitors, and Guest Access

All company sites that allow access to visitors shall track visitor access with a sign in/out log when entering office locations and non-public areas. The purpose for sign-in is to know who is on the premises. All contractors, visitors, and guests must read and sign the AURA Standards of Workplace Conduct. A visitor log shall be used to maintain a physical audit trail of visitor activity at the site as well as computer rooms and data centers and areas where sensitive information is stored or transmitted. The visitor log shall document the visitor's name, the firm represented, and the on-site personnel authorizing physical access on the log, the arrival time, and the departure time. The visitor log shall be retained for a minimum of three months unless otherwise restricted by rule, regulation, statute, or company audit control. Other control measures include the following.

- Visitors shall be identified and given a keycard or other identification that can be deactivated and that visibly distinguishes the visitors from on-site personnel.
- Visitors shall surrender the keycard before permanently leaving the site.
- Visitors shall be authorized before entering and escorted at all times within, areas, where sensitive information is processed or maintained.
- Visitors must be escorted in card access–controlled areas of the facilities.

Government-Mandated Property Survey

Property survey should be made readily available to senior management, Human Resources, and safety professionals to assist in security related events.

Evacuation Plans

Evacuation plans are primarily related to fire safety and should be posted within each building. Additional emergency response information should be included such as whom to call in the event of an emergency.

Government Property

AURA has procedures to control pilferage, destruction, and disposal of government-owned property. Most government property is tagged and documented by AURA property officers. Damage, theft, or loss of property must be reported to the local property officer. All AURA and government property must be turned into Facilities, the property officer, Human Resources, Safety, and/or IT if employment is terminated. A process to account for the recovery of AURA/government property must be established when employment is terminated.

Parking

Guard posts and tiger teeth exits may be provided in some parking areas. Parking on company property is at the employees' risk. The company does not pay for damages caused by other employees or the public; it is, however, recommended that a police report be filed. One parking permit is issued per employee or visitor. Parking permits should not be shared or loaned to others.

Safe Rooms

Safe rooms should be designated at all sites for employees when they make the decision to protect themselves from danger by sheltering in place rather than evacuating. Safe rooms should be located inside the work area; accessible from all parts of the work area; and configured to have at least a solid core door, or door with a small glass panels, a way to restrict vision from the outside, and a way to lock the door and a telephone. Some modifications must conform to fire codes and other health and safety regulations.

Location(s) of the safe rooms shall only be discussed in the workplace security training as to where they are located.

Safe rooms can also be considered for sheltering from some natural disasters.

Alarms

Intrusion alarms detect unauthorized entry during non-business hours. The alarm is usually monitored by a commercial alarm company that contact the local police department and local safety professional to respond and investigate. Sites should consider these types of alarms for areas where sensitive information is being processed.

Duress alarms enable employees to call for help without being obvious to the person causing the problem. The alarm is usually monitored by site Facilities or a commercial alarm company. Persons in duress should, if possible, dial 911 from an office phone and then set down the handset. Sites should consider these types of alarms for reception areas.

Securing a Building (Lockdown)

Buildings may be locked down in a case of a violent situation or on a nearby campus if applicable or for other safety reasons. Site Facilities has the primary responsibility for the following actions when directed by senior management.

- Selected employees should be assigned with the primary and backup responsibility to lock certain doors or areas in the event of an emergency during a shelter in place.
- Assigned employees must have the ability to lock the specified doors. This may be done with keys or by manipulating the door locking mechanism.
- Prepare signs for posting on exterior doors that are locked to tell people what to do. Example: "The building is locked until further notice due to an emergency. Please go to a safe place and try to acquire information from xxx-xxx-INFO or check the website."

Emergency Communications

Anyone that perceives an immediate threat of danger to persons or property or witnesses suspicious persons or activity, should call 911 when in the U.S. or 133 in Chile for assistance.

The local police department and /or fire department will dispatched for immediate response.

When you call 911 or 133, you will be asked the following questions:

- What is happening? This helps the dispatched assign the correct priority response and determine if medical assistance is needed as well.

- Where is the danger? This may not be the same place as from where you are calling.
- Who is causing the danger? (Include a description.) Police will be looking for a dangerous person when arriving at an emergency situation.

Local Site Communication

The ability to communicate emergency information in a single building or work area is crucial to helping protect life and property. Using multiple methods of communication increases the chances of getting the message to larger number of employees. Communication managers should consider the following.

- Implement a local phone tree. Designate primary and secondary staff members as points of contacts to initiate emergency communications. That contact person can call individuals on a prearranged list who would then call a short list of different persons until all employees have been notified.
- Designate primary and secondary staff members in discrete work areas to notify each employee in person.
- When danger is imminent, yell for help or to alert co-workers to evacuate or shelter in place.
- Use a code word or phrase to alert a co-worker to call 911 or 133 when you do not want the suspect or dangerous person to know. The code word or phrase should sound innocuous enough so the person causing the problem does not understand but be common enough that it will not be used accidentally in the course of normal business.
- Other methods for emergency communications such as Slack or WhatsApp
- Email list
- Text messaging
- Intercom or paging systems
- Signing up for campus alert systems if applicable

Identify and Report Concerns

All employees that have identified suspect behavior should report concerns in a timely manner to be proactive to prevent crimes and workplace violence. “If you see something, you should say something.” The key to violence prevention is early identification of concerns and reporting those concerns. Employees should notify their supervisor, or the Head of Human Resources or the Head of Safety, Health, and Environment as soon as possible.

Identify and Discuss Common Scenarios

Each site will have a slightly different concerns and needs. Employees in some workplaces have contact with the public; others have none. Some interact with students; others have less interaction with others. Some workgroups have a large number of employees working in different locations; others have a relatively small group of colleagues. Local site management should have a discussion about known or typical types of concerns and decide on guidelines to handle them.

Assessment and Implementation of an Abatement Plan

After disclosure of a Court Order for Victim Protection or other threats, an assessment may be conducted by Human Resources, Safety, and other senior management. If there is an assessment, an abatement plan will be made in consultation with the affected local managers.

The affected department(s) have the responsibility to implement an abatement plan. The abatement plan may contain elements that may be constrained by the available resources. For example, the physical security of a workplace may be enhanced by changing locks, installing additional lighting, notifying regulatory authorities, and providing increased security services.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this Security Plan as part of normal operations. Examples of acceptable controls and procedures include the following.

- Visitor logs
- Access-control procedures and processes already established
- Operational keycard access and premise control systems
- Operational video surveillance systems and demonstrated archival retrieval of data
- Employee training records related to this plan
- Records of physical inspections related to the requirements of this plan

Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

Distribution

This policy is to be distributed to all staff.

Training Requirements

Training should include the following topics.

Employee Responsibility

The primary responsibility for the security and safety of employees is with each individual employee. The company can help with plans, technology, and training but each employee has to contribute.

The identification and reporting of early warning signs and appropriate intervention is critical to preventing violence.

Recognize and Report Suspicious Persons or Events

While violence does not happen very often, other types of crimes, such as theft, can happen more often. Training on reporting suspicious person(s) or events will help exercise the security plan and prevent some property crimes.

Maintaining Personal Safety

In an emergency, employees should keep themselves safe so they can report the emergency and alert other employees.

Maintain Workplace Security

Each employee should assume responsibility for reporting malfunctions in door locks or equipment to Facilities. Employees should make sure doors close behind them and lock and should not allow unknown person to tailgate behind them when entering a secure area.

Suspicious Persons or Activities

A suspicious person is one that is inappropriately present in an area, such as a private office or nonpublic area, or is exhibiting some unusual or strange behavior, e.g., looking into parked cars and trying door handles. Employees should contact the local Safety professional and Human Resources or, if near campus, press a blue emergency phone if nearby.

Employees do not have to see or recognize a crime before they can call the local Safety professional and Human Resources. A team of members of Human Resources, Safety, and affected senior managers will assess the situation and respond appropriately. Employees will not get in trouble for reporting something that turns out to be legal behavior.

Most thieves who are caught near the time of the crime have been reported by employees who thought the person was suspicious without observing the crime.

Court Order for Victim Protections

Employees are instructed to immediately notify local Human Resources if there are legal actions brought about persons that are somehow related to the employee, whether family or not family.

Confidentiality

Employees should be reassured that their situation will remain as confidential as possible, consistent with AURA's responsibility to maintain a safe workplace, and that other parties may be contacted on a need-to-know basis in order to maintain a safe workplace.

Response to Violence

The Security Plan is devoted to identifying and addressing early warning signs to prevent violence and to having physical and training resources in place to react more effectively if violence occurs. This part of the Security Plan addresses the immediate actions that are necessary to take when violence is happening right now.

Evacuate or Shelter in Place?

There are two primary choices of actions to take when confronted by violence.

If it is dangerous to stay in an area/room/building, evacuate (RUN AWAY). This is when the source of danger is close to you but does not control escape routes.

- Violence nearby but it is possible to leave
- Get to a Safe Location
- Call for Help dial 911 in the US or 133 in Chile

If it is dangerous to leave the area/room /building, Shelter in Place (Securely HIDE OUT). This is when the source of danger controls or blocks access to escape or you do not know the location of the sources. "Securely HIDE OUT" means

- Go to locked or barricaded room with limited visibility from outside and with telephone;
- get down on the floor and out of the line of fire;
- call for help by dialing 911 in the U.S. or 133 in Chile; and
- wait for official notice that the danger is over.