BIOSECURITY PLAN

-

Updated 02/08/2021

This is the written biosecurity plan for the University of Arizona. This plan addresses and meets the requirements of the Select Agent Regulations.

THE UNIVERSITY OF ARIZONA
Research
Research Laboratory & Safety Services

TABLE OF CONTENTS

Certification and Approvals

This Biosecurity Plan has been approved by:

James Spencer, MS, RBP
Biological Safety Officer

This Biosecurity Plan for the University of Arizona has been prepared in compliance with the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* and 7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part 73. This plan was organized based on information provided in the *APHIS/CDC Select Agent and Toxins Security Information* Document from March 8, 2007. This plan is required to be reviewed annually and updated whenever changes occur. The signature below verifies the annual review for this plan was completed.

08Feb2021

Signature of Biological Safety Officer **Date**

James Spencer, MS, RBP

Research Laboratory & Safety Services (RLSS)
1717 E. Speedway Blvd. (Bldg. 151)
Suite 1201
Tucson, AZ 85724
P.O. Box 245101
www.rlss.arizona.edu
Phone (520) 626-6850 Fax (520) 626-2583

For emergency assistance after hours,
call University Police at 621-UAPD (621-8273)

Site-Specific Risk Assessment

The following information is based on Site Specific Risk Assessments provided by the University of Arizona Police Department (UAPD). See Appendix A for further information.

Using the definitions and considering all the threats listed, the following was determined:

The overall agent-specific risk for the entity is:

Low
Moderate
High
Highest

The probability of a listed threats occurring is:

Man: Moderate Nature: Low Incident: Moderate

The overall consequences if a threat should occur are:

Man: Moderate Nature: Low Incident: Moderate

Consistent practices of safety and security techniques enhance overall security of the areas.

Vulnerability Assessment

The overall vulnerability is:

Low
Moderate
High

Graded Protection (Mitigation Measures)

Considerations: Physical security includes any device or protection measures that limit access to select agent activity or storage areas starting from the select agent activity area and working outwards. Devices used include locks on storage units, locks on laboratory doors, electronic monitoring systems (including CCTV), card-key access, PIN access, fingerprint access, etc., in any combination. Physical barriers include laboratory walls (floor to ceiling), a room within a room, secured storage rooms, secured storage units, building perimeter walls and fences, security guards, security patrols, etc., in any combination.

Physical Security

All laboratories are required to store recombinant and/or biohazardous materials within a secure space. If materials are outside their designated storage area they must always remain under line of sight. If a breach in physical security is discovered, it must be reported to UAPD and the BSO/ABSO immediately.

If laboratories with access control systems fail (i.e. key card reader, panel, access control operating systems), then access to the spaces will not be possible. This ensures the door(s) have a fail secure ability, with the only way to access the space being with a hard key that is only accessible by designated individual(s).

Information Security and Routine System Updates

The University of Arizona has an Information Security Office (ISO) that coordinates updates, news, and security issues directly to the IT & Program Developmental Manager in RLSS.

RLSS has a central patch server that connects to all the RLSS computers and pushes patches automatically, but a critical patch can be scheduled as needed.

The building management system for Keating is patched on a routine schedule that occurs monthly. Critical patches are done immediately when needed.

Information Systems Controls

- If you are accessing the RLSS network from an off campus location, you are required to use two (2) factor authentication. This requires University of Arizona NetID password and a second form of authentication (i.e. a mobile device, NetID +).

- The servers that support the RLSS CHESTER system are maintained in a locked cabinet, in a room with keycard access. The building is also secured with an active alarm system when it is unoccupied.

- Individuals not employed with RLSS are given limited access to electronic information via the User Dashboard. The authentication process is based on the NetID system at the University of Arizona. Access is automatically removed once their position in the University of Arizona is terminated.

Understanding and Complying with Security Procedures

All individuals authorized to work with recombinant and/or biohazardous material shall review and be familiar with this document. These individuals must also be knowledgeable of the mechanisms in place to contact UAPD in the event of an emergency.

Individuals working alone in the BSL-3 suite have access to an emergency pager, and its use is recommended during these times. The pager must be stored within the BSL-3 suite, in an easily accessible locations near the main entry.

Reporting Requirements to the Biological Safety Officer

The following must be reported immediately to the BSO/ABSO:

- Any loss or compromise of keys, key cards, passwords, combinations, etc.
- Any suspicious persons or activities near or inside laboratories.
- Any suspicious activity that may be criminal in nature.
- Any loss or theft of recombinant and/or biohazardous material.
- Any release of recombinant and/or biohazardous material outside of primary containment.
- The isolation of a non-authorized select agent or toxin from a diagnostic sample.
- The delivery of an unexpected package containing recombinant and/or biohazardous material.
- Any event where the security of a recombinant and/or biohazardous material is in question.

Once reported, the BSO/ABSO will take action to make all appropriate notifications and complete all forms, including the required follow-up.

Any event that would trigger a response by the University of Arizona Critical Incident Response Team (CIRT) must be reported. RLSS is the office of the BSO/ABSO and can be contacted at (520) 626-6850 during office hours. After office hours, all security issues must be reported to the UAPD at (520) 621-8273 or 9-1-1. Once reported, the UAPD will notify the BSO/ABSO, and appropriate action will be taken to inform federal, state, and local law enforcement agencies as needed.

Access Approval and Control

When an individual requires access, the Approval Holder (AH) and/or Approval Safety Coordinator (ASC) will add the new worker to their Biosafety approval using the RLSS User Dashboard. The individual is required to complete all applicable training, including laboratory specific training, prior to having unescorted access to the laboratory space. Some laboratory spaces will require the building manager to help the individual in setting up a PIN and fingerprint access. Individuals are required to never share their unique means of access (such as passwords, PIN numbers, keys, and key cards).

When an individual leaves the university, or no longer requires access to a specific space, the AH or ASC request removal of the worker from their Biosafety approval using the RLSS User Dashboard. If needed, the building manager will remove the individual's access to the laboratory space by disabling PIN and/or fingerprint access.

Personnel with access to a laboratory space can escort other individuals into the spaces that do not currently have access. The escorted individuals must sign the visitor access log before entering the space and must agree to all terms of being escorted into the space, which will be explained to them by the escort. The escort must ensure that the escorted individuals follows all rules including wearing proper PPE for the area they are entering, donning and doffing procedures, and staying in the line of sight of the escort at all times. The escort should also ensure that whenever entering a PIN, that they shield this from the escorted individual. If any escorted individual is found to have not followed the instructions of the escort, the deviation should be reported to the BSO/ABSO as soon as possible.

Public Access Areas

Laboratories are inaccessible to the public, located in secured buildings, and require specific security enter requirements (Fingerprint/key card). All visitors to laboratories must sign in after entering and must be always escorted. The escort(s) must always have a line of sight on every person being escorted into the laboratories. The emergency contact information for the UAPD, RLSS, BSO/ABSO, and for specific individuals in charge of the laboratory space will be posted inside the space.

Unauthorized or Suspicious Persons

Personnel are required to question unauthorized or suspicious persons in and around the laboratory. If the individual determines that the suspicious person does not have the need to be in the area, they should ask the person to leave and escort them out of the area. Suspicious individuals and suspicious activity that may be criminal in nature, or individuals that refuse to leave, are required to be reported immediately to the UAPD, BSO/ABSO, and other management (i.e. building manager, PI) as appropriate. UAPD will help remove the suspicious individual from the area, take a report, and may request that the individual not return to the area without an escort, or not return at all. If it is determined that the individual should not return to campus altogether, UAPD will place them on the list of restricted individuals that is sent out to all security personnel and available for public view on the UAPD website.

Loss or Compromise of Keys, Passwords, or Combinations

In the event of a loss or compromise of keys, passwords, and/or combinations, the BSO/ABSO should be notified immediately. The BSO/ABSO may request that all access to the spaces be suspended until the incident is addressed. Combinations or passwords that have been compromised need to be changed as soon as possible, and those needing the new combination or password notified.

Access Control System Inoperability

In the unlikely event that the access control system becomes inoperable, there are measures in place to enter/exit the space until the system is operable again. Each space has a key(s) that can be used to manual open the door if the electronic control systems are non-functioning. These keys are kept in a secure area that are only accessible by the building manager of the space, and they are contacted in the event that the door(s) will not open. The doors are set to a "failed secure" setting so that even if the electrical control system fails, the doors will not be able to be opened from the outside with a key. In the event that laboratory personnel need to access the area while the control system is down for experimental purposes (ex: time points, animal checks, etc.), an authorized person can be stationed outside the door to let specific individuals into the space. These authorized individuals would include UAPD, BSO/ABSO, or the building manager, and they would be responsible for checking identification prior to the individual being given access to the space. They will also need to document the name, date, and time that that individual access the space, since the records management system would also be non-functioning at this time. These measures will remain in place until the system is back to functioning as designed.

An electrical outage is an area of concern for the BSL-3 space(s), and could affect the functioning of the access control, security monitoring, and records management systems. In the event of any electrical failure, the spaces are connected to emergency generator systems. There is also a backup battery system (4 hours of power) in the event that the emergency generator does not kick on, or runs out of power. The batteries are replaced every two years, and the emergency generator undergoes preventative maintenance to ensure it is functioning properly.

Inventory Control and Securing Select Agents and Toxins

Recombinant and/or biohazardous material storage areas are isolated from public access. These spaces must be secure to ensure no unapproved access occurs, and materials must be stored inside secure freezer units in the designated storage space. An entry log maybe required for specific spaces, and if so, must be maintained. An entry log should document the name, date, time, and reason for accessing materials each time the storage area is accessed. The inventory logs should be maintained by the AH or AH's designee, and available at all time for review by RLSS. If any alteration to the inventory records is observed or suspected, or a discrepancy is noticed during an inventory, the BSO/ABSO must be notified immediately so an investigation can be initiated.

Maintenance and/or Repairs

If maintenance or repairs are required on any of the equipment in a space, or on the space in general, the workers must be escorted by laboratory personnel with unescorted access. Unescorted individuals must always keep eyes on the escorted personnel and follow all other rules for escorting visitors into the space.

Inventory Records

Records relating to physical inventory and the destruction or transfer of physical inventory must be maintained by the AH or AH's designee. These records must be kept readily available for inspection by RLSS.

Retention of Records

Records relating to security are retained for three (3) years and include the following:

- Inventory transfers.
- Theft, loss, and/or release of recombinant and/or biohazardous material.
- BSO’s records pertaining to biosecurity, biosafety, and/or incident response events.

Appendix A: Emergency Contact Information

University of Arizona Police Department – (520) 621-8273 or 9-1-1
Fire, general emergency - 9-1-1

All university phones will contact UAPD directly. If calling from a cell phone, give your identity and location, and you will be immediately connected with UAPD.

Research Laboratory and Safety Services – (520) 626-6850

Biological Safety Officer: **James Spencer** – Cell: (443) 375-7393

Assistant Biological Safety Officer: **Ceasar Ramirez** – Cell: (520) 309-8955

Risk Management and Safety – (520) 621-1790

Appendix B: Site Specific Risk Assessments

Threat Vulnerability Assessments - January 4, 2008, April 22, 2009, March 25, 2010, U.S Department of Homeland Security Evaluation in May 2010

Thomas W. Keating Bioresearch Building
1657 E. Helen Street
Tucson, AZ 85721

Threat Vulnerability Assessments – May 6, 2009, March 25, 2010

Central Animal Facility
1127 E. Lowell
213/215

Threat Vulnerability Assessments – April 21st, 2009, February 23, 2010

Arizona Health Science Center
1501 N. Campbell
1256/1256A