BIOSECURITY PLAN

Updated 04/19/2019

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

Site-Specific Risk Assessment ........................................................................................................ 1
Physical Security ............................................................................................................................ 2
  Information Security and Routine System Updates ................................................................. 3
  Information Systems Controls ................................................................................................. 3
Understanding and Complying with Security Procedures ......................................................... 3
Reporting Requirements to the Responsible Official ................................................................. 4
Access Approval and Control ...................................................................................................... 4
Public Access Areas .................................................................................................................... 5
Unauthorized or Suspicious Persons .......................................................................................... 6
Loss or Compromise of Keys, Passwords, or Combinations ..................................................... 6
Receiving Select Agents and Toxins ............................................................................................ 6
Intra-entity Transfers .................................................................................................................. 7
Shipping Select Agents and Toxins ............................................................................................ 7
Inventory Control and Securing Select Agents and Toxins ....................................................... 7
Inventory Records ...................................................................................................................... 8
Retention of Records .................................................................................................................. 8
Drills and Exercises ..................................................................................................................... 8
Select Agent Reference Document ............................................................................................ 8
Appendix A: Emergency Contact Information .......................................................................... 9
Appendix B: Site Specific Risk Assessments ............................................................................. 10
Certification and Approvals

This Biosecurity Plan has been approved by:

James Spencer, MS, RBP,
Responsible Official
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.

Signature of Responsible Official: [Signature]
Date: 04-19-2019

James Spencer, MS, RBP

Research Laboratory and 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.

This assessment is in accordance with Centers for Disease Control and Prevention (CDC) Security Plan Guidance and Information Systems Security Controls Guidance documents. 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

The threat assessment as determined by the nature of the open-lab design requires that entries to Select Agent & Toxin (SA/T) laboratories are proximate to non-select agent activities. However, security measures reduce vulnerability. 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.

**Entity Security Consensus Meeting**

Relevant staff members have met and concluded based upon the agent, threat, and vulnerability assessments the following security measures are necessary to prevent the theft, loss, and release of SA/T:

1. Access to the floors where the registered spaces are located require a keycard for the elevator and stairs. Room keys and biometrics are located at the entrance to the registered spaces.
2. Video surveillance cameras located in the registered spaces entry points.
3. Motion detectors in selected interstitial spaces above specific areas of ceilings.
4. Freezer(s) used to store SA/T are kept locked at all times, and the key(s) are stored in a separate location.

**Physical Security**

All laboratories are required to store SA/T within a locked container inside a secure, alarm monitored registered space. If the SA/T are outside their designated storage area it must remain under line of sight at all times by an Security Risk Assessment (SRA) approved individual. If a breach in physical security is discovered, it must be reported to the RO/ARO immediately.

If the 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 SRA 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
- Hard copies of records entailing SA/T information are kept in a secure area, until they are able to be shredded. All electronic data entailing SA/T information is secured from outside user access. All individuals that are hired and assigned to duties involved with handling SA/T in registered spaces, or SA/T information, are required to have a current SRA approval. This approval must be complete prior to being given unsupervised access to anything related to SA/T. All electronic SA/T related data must be protected by a firewall that does not allow unauthorized or outside access. RLSS staff log in requires an authentication process prior to accessing any data, and their access is revoked immediately upon termination of their position.

- 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, but are SRA approved, 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, or they no longer need to access SA/T.

Understanding and Complying with Security Procedures
All individuals authorized to work with SA/T 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 Responsible Official**
The following must be reported immediately to the RO/ARO:

- Any loss or compromise of keys, key cards, passwords, combinations, etc.
- Any suspicious persons or activities near or inside SA/T laboratories
- Any suspicious activity that may be criminal in nature
- Any loss or theft of select agents or toxins
- Any release of a select agent or toxin 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 select agents or toxins
- Any event where the security of a select agent or toxin is in question

Once reported, the RO/ARO 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 RO/ARO 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 RO/ARO, and appropriate action will be taken to inform federal, state, and local law enforcement agencies as needed.

**Access Approval and Control**
To work with SA/T and access registered spaces, personnel must receive a Security Risk Assessment (SRA) approval and be listed on the Centers for Disease Control and Prevention (CDC) Form 1, Section 4, Entity Personnel.

When an individual requires access, the principal investigator will inform the Responsible Official or the Alternate Responsible Officials (RO/ARO) to initiate the process. The RO/ARO requires a completed FD-961 with fingerprints from the individual needing access. They will then submit the request to the CDC/FBI so that a background check can be initiated. Once the approval has been received from the CDC/FBI, the individual and their PI(s) are notified by the RO/ARO. The RO/ARO will then provide training to include the biosafety, biosecurity, incident response, and agent specific information. After the training is complete, the individual can request access to the spaces from the building manager, who will confirm with the RO/ARO that the individual has a current SRA and training. The building manager will help the individual in setting up a PIN and fingerprint access for the registered spaces since they control keycard access to the spaces. Individuals are required to never share their unique means of access (such as passwords, PIN numbers, keys, and key cards) to registered areas.
When an individual leaves the university, or no longer requires access to SA/T, the PI will notify the RO/ARO and the building manager. The building manager will remove the individual’s access to the registered spaces, and the RO/ARO will remove them from the CDC Form 1.

Personnel with a current SRA can escort other individuals into the registered spaces that do not have a current SRA and access to the spaces. The escorted individuals must sign the 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 SRA escort. The escort must ensure that the escorted individuals follows all rules to include not handling any SA/T, access is not allowed in areas with active SA/T work, 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 RO/ARO as soon as possible.

When no SA/T are in use, registered rooms may be used for other purposes with approval from the RO/ARO. For this to happen, all SA/T are removed from the space, surfaces and equipment are decontaminated using 10% bleach for 15 minutes (or other approved methods), and the decontamination documented and maintained for records. Once the decontamination is complete, the RO/ARO are notified and can approve the space to be used for other purposes. PI(s) will notify the RO/ARO at least 60 days in advance of when the space will need to revert back to housing SA/T so preparations can be made and staff can be notified. Prior to reverting back to handling SA/T in the space, the building manager, PI, and RO/ARO will meet to ensure that all procedures are back in place, and access is again only granted to individuals with a current SRA. Once everything has been confirmed to be back in place, the SA/T can be moved back into the registered space.

Electronic access control logs are sent to the building manager and RO/ARO monthly by the building security company. These records are stored on a shared drive by the RO/ARO so they can be reviewed when needed.

**Public Access Areas**

All SA/T laboratories are inaccessible to the general public, are located in secured buildings, and require specific security enter requirements (Fingerprint/key card). All visitors to the SA/T laboratories must sign in after entering the anteroom, and must be escorted at all times. The escort(s) must have a line of sight at all times on every person being escorted into the SA/T laboratories. The emergency contact information for the UAPD, RLSS, RO/ARO, and for specific individuals in charge of the laboratory space will be posted inside the SA/T space.
Unauthorized or Suspicious Persons
SRA approved individuals are required to question unauthorized or suspicious persons in and around the select agent use/storage area(s). Suspicious individuals and suspicious activity that may be criminal in nature are required to be reported immediately to the UAPD, RO/ARO, and other management (i.e. building manager, PI) as appropriate. SRA approved individuals are responsible for checking the credentials of any individual they are not familiar with prior to escorting them into the laboratory. If there are any questions regarding a person’s need to access a registered area, contact the RO/ARO prior to escorting the individual. All of these reporting requirements are covered in annual SA/T training given by the RO/ARO.

Loss or Compromise of Keys, Passwords, or Combinations
In the event of a loss or compromise of keys, passwords, and/or combinations, the RO/ARO should be notified immediately. If a physical key to an area where SA/T are used or stored is lost, the building manager will be notified by the RO/ARO so that a new locking mechanism can be installed urgently. The RO/ARO may also request that all access to the registered spaces be suspended until the new locking mechanism has been installed. Combinations or passwords that have been compromised need to be changed as soon as possible, and those needing the new combination or password notified.

If a physical key to a freezer where SA/T is stored is lost, the door to the room will become the locking point since the room is keycard and fingerprint access. The RO/ARO may also request access to the freezer room be suspended until the problem is resolved. The freezer will be physically secured by mechanical means until it is rekeyed, replaced, or alternatively secured. A new inventory of SA/T will be conducted prior to the issuance of new combinations or keys for the freezer storage room.

Receiving Select Agents and Toxins
When a SA/T shipment is received from an external-entity, the shipment must be secured as soon as possible in an approved SA/T space. The shipment should be unpackaged in a manner to ensure that the agent is not damaged in any way. The agent should then be secured in an appropriate storage space, the RO/ARO notified of safe arrival of the package, the inventory of the laboratory updated, and all appropriate documentation for the arrival of the agent completed.

The recipient must immediately notify CDC/USDA, RO/ARO, and relevant PI if the select agent or toxin has not been received within 48 hours after the expected delivery time, or if the package containing SA/T has been damaged to the extent that a release may have occurred.

Unexpected shipments of a SA/T must be secured immediately upon arrival in a SA/T approved space, and the RO/ARO notified. The individual taking receipt of the package will rely all information known about the package to the RO/ARO, so they can contact
the CDC. The RO/ARO will assume responsibility for the package until a determination can be made about what steps should be taken.

**Intra-entity Transfers**
All intra-entity transfers at this facility will be overseen by the RO, who will ensure that a facility intra-entity transfer form is properly completed. This will include ensuring the transferred SA/T is accurately reflected in the inventory of both laboratories. The physical transfer of the SA/T, will be performed by two individuals with an active SRA. All biosafety and security provisions will be discussed with the RO/ARO prior to any intra-entity transfer at this facility. UAPD escort may be necessary to ensure that transfers are conducted in a secure manner (e.g., between floors, buildings, etc.).

**Shipping Select Agents and Toxins**
A SA/T may only be transferred to individuals or entities registered with APHIS/CDC to possess, use, or transfer that specific SA/T. APHIS/CDC Form 2 is used to document transfers to or from other institutions with a certificate of registration from CDC or APHIS. All external-entity transfers will be handled by the RO/ARO, who will ensure that both entities have the proper and accurate documentation needed to transfer and accept SA/T. A valid APHIS/USDA permit may be required when shipping animal or plant pathogens. The RO/ARO will ensure that the University of Arizona, and the external-entity receiving the pathogen have proper and accurate documentation.

PIs or designated staff with a current SRA will ensure proper secure packaging and inventory control for agents being shipped between the University of Arizona and other external entities. Any staff involved in the packaging/shipping of SA/T must be current in DOT/IATA shipping training offered by Risk Management Services. All packages, containers, carts, bags, and briefcases that will be removed from a SA/T approved space must be inspected by an SRA approved escort. All biosafety and security provisions will be discussed prior to any external-entity transfers being initiated. UAPD escort may be necessary to ensure that transfers are conducted in a secure manner (e.g., between floors, buildings, etc.).

Commercial carriers selected to conduct the shipping of SA/T must meet U.S. Department of Transportation hazardous materials regulations. The package containing select agents/toxins must be labeled generically as “Category A Infectious Substances”, and contain all other appropriate labeling.

**Inventory Control and Securing Select Agents and Toxins**
Select agent areas are isolated from public access, and can only be under the control by personnel who hold a current SRA. These spaces are registered with the CDC as select agent areas, and must be locked and monitored at all times by security systems to ensure no unapproved access occurs. Select Agents are stored inside lockable freezer units in the designated storage room, and the key to these units is stored in separate location inside the BSL-3 suite. An entry log is maintained for the locked freezers that records
name, date, time, and reason for access that must be filled out each time the units are opened. The inventory logs are maintained and secured by SRA approved laboratory personnel, and must available at all time for review by the RO/ARO. If any alteration to the inventory records is observed or suspected, or a discrepancy is noticed during an inventory of stored SA/T, the RO/ARO must be notified immediately so an investigation can be initiated.

The select agent laboratory has a motion-activated alarm in selected interstitial spaces above specific areas of the ceiling. Alarms and video cameras can be monitored by the building manager, who holds a current SRA.

**Inventory Records**
Records relating to physical inventory and the destruction or transfer of physical inventory must be maintained by the PI or PI’s designee as stated on the Form1. These records must be kept readily available for inspection by the RO/ARO. The RO/ARO must document the annual inspection when SA/T are stored on site.

**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 SA/T
- RO’s records pertaining to biosecurity, biosafety, and/or incident response events

Outdated and/or unneeded records shall be shredded by the RO/ARO.

**Drills and Exercises**
Drills and exercises conducted at this facility that satisfy the requirements of the Biosafety, Biosecurity, and Incident Response Plans are conducted on an annual basis and the drills conducted by this facility are summarized in an annual drill document. Written plans at this facility are updated annually and when drills and exercises warrant updating.

**Select Agent Reference Document**
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
Responsible Official: James Spencer – Cell: (443) 375-7393
Alternate Responsible Official: Charles Schable – Cell: (520) 204-4766

Laboratory Personnel
Principal Investigator: Dr. Janko Nikolich-Zugich – Office: (520) 626-6065, Cell: (503) 481-9776

Laboratory Manager: Jennifer Uhrlaub – Office: (520) 626-0554, Cell: (520) 850-1716

Principal Investigator: Dr. Linda Powers – Office: (520) 621-7634, Cell: (520) 343-2090

Keating Building Manager, Robert Sandoval – Office: (520) 626-8512, Cell: (520) 275-7603

Director, University Animal Care: Dr. David Besselsen – Office: (520) 626-1066, Cell: (520) 349-7897

AHSC Senior Husbandry Manager: Cheryl Johnson – Office: (520) 626-6270, Cell: (520) 419-6415

AHS Husbandry Coordinator: Miguel Diaz – Office: (520) 626-6706, Cell: (520) 419-6413

Risk Management and Safety – (520) 621-1790
Appendix B: Site Specific Risk Assessments


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

All additional threat vulnerability assessments of SA/T Labs will be placed here.