

## SECURITY ADVICE FOR RESEARCH FACILITIES

---

### References

This SOP is derived from the following documents and guidelines:

- **UNL Biosafety Guidelines** rev. 2018 (ver. 2.0). UNL Environmental Health and Safety;
- **Biosafety in Microbiological and Biomedical Laboratories (BMBL; 5<sup>th</sup> ed.)** Center for Disease Control and Prevention, National Institutes of Health.

### Introduction

Research security is an integral part of an effective biosafety program. Bio-security goals include the following:

- Prevent loss, damage, or contamination of valuable teaching and research materials and/or related sensitive information;
- Prevent release of potentially harmful organisms into the environment;
- Prevent accidental exposure to faculty, staff, students, and visitors; and
- Reduce the risk of theft of biohazardous material for malevolent purposes.

Where applicable and possible, security measures should also be followed during analogous field research projects.

When a biosecurity plan is implemented, it should be reviewed on a regular basis for effectiveness, and should reference relevant UNL policies and plans.

### Scope

Security policies, practices, and procedures in this SOP apply to all UNL research facilities engaged in the following types of approved projects:

- Work with animals (includes sampling wild animal populations);
- Projects involving recombinant or synthetic nucleic acids (r/sNA) conducted at Biosafety Level 2 and Biosafety Level 3 containment.
- Genetically-modified whole organisms (i.e., animals, insects and plants)
- Projects involving Risk Group 2 (RG2) or Risk Group 3 (RG3) infectious agents and toxins.



*Projects or experiments involving the use of human, animal, or plant pathogens, and/or r/sNA require submission and approval of an IBC protocol. Please see the UNL Biosafety Guidelines for additional information. Work with research animals also requires submission and approval of IACUC protocols.*

## **General Security Measures**

Employees, as day-to-day occupants of research spaces, provide the first line of laboratory security.

- Laboratory access should be restricted to those with a need; the PI is responsible to determine who will be granted access rights. Key card access (when available) can be a valuable tool to help ensure proper access privileges
  - Keep laboratory doors closed as much as possible. This protects experiments from potential contamination and discourages individuals from entering unnecessarily. Lock the doors when the room is unoccupied.
  - Contact Building Maintenance (BSM) promptly to remedy compromised security features, such as broken locks and arrange for alternate security measures until repairs are complete.
  - Keep stocks of samples and microorganisms locked during off hours and when not attended by laboratory personnel. Freezers and refrigerators in corridors and shared spaces are particularly susceptible to access, so they should be locked at all times.
  - Do not leave keys or access cards in open or accessible areas. Do not disclose access codes or loan keys to other personnel. Limit the number of persons with access rights to the minimum required to conduct the work in an efficient manner.
  - Unauthorized personnel should be asked to leave the research area. If you do not feel comfortable with someone's presence, be prepared to take appropriate action. Your approach should be to:
    - a) ask them if they need assistance;
    - b) politely ask them to leave the area;
    - c) ask them to follow you to the department office to seek information (but do not leave the area unsecured while you serve as the escort);
    - d) if necessary, call the UNL Police for assistance.
- Report such occurrences to the UNL Police Department.
- Discuss how to handle strangers beforehand so that your response is proper and effective. The UNL Police can provide training and additional information upon request.
  - Know the facility schedule for locking doors, gates, or other access points. If unauthorized people are present in the area after it has been secured, call the UNL Police.
  - Visually inspect all packages of biohazardous materials arriving at the work area and open them within a certified biological safety cabinet. If stains are present on the package, the package is unexpected, or the package is damaged, isolate

2

*(Created 12/01; Revised 7/04, 6/08, 12/15)*

and secure the package, do not open it, and call the UNL Biosafety Officer or EHS. Packages shipped out using a commercial vendor (FedEx, etc.) must be prepared in accordance with applicable DOT/IATA regulations and offered for shipment only by personnel who have completed shipping training within the past three years (Designated Shippers).

- PIs who maintain stocks or collections of human, animal, or plant pathogens are required to prepare and maintain a Pathogen Inventory (please see the EHS SOP "Pathogen Inventories" for additional information). Report any losses to the UNL Police and the Biosafety Officer/EHS. Promptly decontaminate and discard unnecessary stocks and notify EHS of abandoned stocks of biohazardous materials.
- Biohazardous waste items related to RG-2 and -3 organisms, or r/sNA must be properly decontaminated before disposal. This is easily accomplished by autoclaving. Also, ensure that autoclave areas are monitored. Please reference the EHS SOPs **Autoclave Operation and Performance Testing** for proper autoclave operation and, **Disposing of Biohazardous Materials including Recombinant Nucleic Acids** for acceptable waste disposal methods.
- At the end of every work session, ensure that all biological materials have been properly stored and secured. Ensure all access doors are locked.

### **Cybersecurity Measures**

In addition to physical security measures, cybersecurity is just as important to guard against research being accessed by unauthorized individuals.

- Ensure computer passwords are strong, containing at least 8 characters, and at least one of the following: uppercase letter, lowercase letter, number, and symbols.
- Do not post computer passwords in the lab or office areas.
- Do not open emails from unknown sources on lab computers.
- Change computer passwords to common lab computers when staff changes occur.

### **Threat Awareness**

The measures described above are good general security measures that are easy and simple things to ensure the lab and lab data are secured. However, sometimes the threat does not come from an obvious source. The following tips are intended to help you identify security threats from unusual sources.

- Insider Threats – Following are examples of suspicious behavior that should be reported.
  - Sudden changes in work habits/hours
  - Secretiveness
  - Suspected substance abuse
  - Conflicts with coworkers

- Outsider Threats – Following are examples of suspicious behaviors that should be reported.
  - Asking detailed questions about your place of work
  - Asking detailed questions about your research
  - Lurking outside building entrances
  - Unusual cars parked in parking lot overnight
  - Persons taking pictures outside your place of work.

Any suspicious activities should be reported to your supervisor and UNLPD (402-472-2222).

### **Additional Considerations**

Additional security measures may also be appropriate based on research or organism specific considerations. Applicability and appropriateness of additional security measures should be determined by the Principal Investigator using a risk assessment approach. Regulatory agencies such as USDA-APHIS and HHS/CDC may also recommend or require security enhancements to limit access to materials and agents that require special permits to possess.

Submission of a complete protocol for review by the IBC includes questions to evaluate if the research could be considered dual-use, that which has a potential for bioterrorism applications. In addition, the 5<sup>th</sup> Ed. of the BMBL describes a risk assessment approach that considers the biological agents in possession relative to potential for misuse and potential consequences; insider and outsider threats, motivation, and opportunity; robustness of existing security measures; and the need for enhanced measures.

### **BSL 3/ABSL-3 Security Measures**

Each BSL-3 containment facility must have an individual security plan, and the plan must be based on a security and vulnerability assessment. The plan must be developed with input from the PI, EHS, administrative officials, and UNLPD, at a minimum. When work with select agents is anticipated, the plan must also conform to all applicable regulatory requirements, including periodic drills.

### **If Security Is Compromised**

If you believe security of your lab or facility has been compromised, contact your supervisor immediately. Together you should contact UNLPD and the Biosafety Officer and they can assist you with filing a report and putting temporary security measures in place until the security breach is located and fixed.