

Bio Security Plan

Purpose and Introduction

There are specific rules and regulations that govern the use of certain biological agents and toxins ("select agents"). The USA Patriot Act of 2001 established criminal penalties for possession of certain biological agents and toxins if used as a weapon or for any reason not reasonably justified for prophylactic, protective, bona fide research or other peaceful purposes (select agents <http://www.selectagents.gov/>). The Act established certain controls over select agents to ensure that no "restricted person" transports, ships or possesses select agents.

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PHSBPRA) greatly expand control of possession, transport and use of select agents.

PHSBPRA mandates the following:

- The formation of lists of biological agents and toxins that have the potential to pose severe threats to the public's health and safety by the U.S. Department of Health and Human Services (HHS) and the Department of Agriculture (USDAA)
- The promulgation of regulations by HHS and USDA establishing the following: safety measures for select agents including proper training and appropriate skills to handle select agents and proper laboratory facilities to contain and dispose of the agents; the security of select agents to prevent their use in domestic and international terrorism; procedures to protect the public safety in the event of the transfer of such materials in violation of the act; and ensure the availability of biological agents and toxins for research, education and other legitimate purposes
- The promulgation of regulations by HHS and USDA for the possession, use and transfer of select agents, registration of individuals including provisions to ensure that persons registering have a lawful purpose to possess, use and transport the agents; and procedures to identify and characterize the agents held at a facility
- Prompt notification of the release of a select agent outside the biocontainment area
- The promulgation of regulations by HHS and USDA to ensure that appropriate safeguards and security arrangements for persons possessing, using or transferring the agents exist at a facility. Registered persons shall have their names and other identifying information submitted to the Department of Justice (DOJ). Access shall be denied to those identified as restricted persons; access shall be granted to only those individuals identified by the Secretaries of HHS and USDA and DOJ; the DOJ shall use criminal, immigration, national security and other electronic data bases to determine if a person is a restricted person or otherwise suspected of committing a crime, being involved in an organization that engages in domestic or international terrorism, or being an agent of a foreign power.
- Establishes penalties for violation of the Act.

Federal Regulation, 42CFR73 "Possession, Use & Transfer of Select agents & Toxins, Final Rule," mandates that an entity develop and implement a security plan establishing policy and procedures that ensure the security of areas containing select agents and toxins.

The security plan must be based on a systematic evaluation in which threats are defined, vulnerabilities are examined and risks associated with those vulnerabilities are mitigated with a security systems approach.

The NC State University Biosecurity Plan specifies security requirements for NC State University laboratories using select agents. The NC State University Biosafety Committee recommends that all users of biological agents consider adopting the requirements outlined in this Biosecurity Plan.

Responsibilities

Responsible Official (RO)

- Develop and implement safety, security and emergency response plans
- Allowing only approved individuals to have access to select agents or toxins
- Providing appropriate training for safety, security and emergency response
- Assures that transfer of select agents or toxins is done according to the rules of the Act
- Provide timely notice of any theft, loss or release of a select agent or toxin
- Maintain detailed records of information necessary to give a complete accounting of all activities related to select agents or toxins
- Report the identification of a select agent or toxin as a result of diagnosis, verification or proficiency testing
- Conduct regular inspections, at least annually, of the laboratory where select agents or toxins are stored or used to ensure compliance with all procedures and protocols of the safety plan. The results of these inspections must be documented and any deficiencies must be corrected.

Alternate Responsible Official (ARO)

The ARO must meet all the qualifications for the RO and must be able to conduct all the activities of the RO in the absence of the RO

Select Agent User

- Maintain a log of select agent stock quantities stored – select agent identification; storage location; amount stored; date; initial of person doing entry.
- Maintain a use log of select agent and reconciliation – amount used; date, initials of user.
- Will report to the Responsible Official or Alternate Responsible Official:
 - Any loss or compromise of their keys, passwords, combinations
 - Any suspicious persons or activities
 - Any loss of theft of select agents or toxins
 - Any release of select agents or toxins
 - Any sign that inventory and use records of select agents or toxins have been altered or otherwise compromised.
- Allow unescorted access only to approved individuals who are performing a specifically authorized function during hours required to perform the defined job.
- Allow individuals to conduct routine non-laboratory functions only when escorted and continually monitored by approved individuals
- Will report to the RO/ARO all select agents used
- Will notify the RO/ARO of all authorized personnel to use select agents or toxins.

Inventory Control Procedures

The select agent user must keep a record of the agents location, how it is used, inventory, transfers – external/internal and destruction and access.

Copies of logs will be provided to the RO/ARO during inspections. Researcher will keep record of logs indefinitely.

The following logs are required:

- Name, characteristic and source date of agent
- The quantity acquired, the source and date of acquisition
- Quantity held on the date of the first inventory (toxin only)
- Current quantity held (toxin only)
- The quantity used and dates of the use (toxin only)
- The name of each person who has accessed any select agent or toxin
 - The select agent or toxin used
 - Date removed
 - The amount of toxin used
 - The date agent was returned to storage
 - Quantity of toxin returned
- The quantity transferred, transfer date, recipient's name

Shipping must conform to applicable regulations. Prior to shipment, contact the University Biosafety Specialist for instructions. The Biosafety Specialist will provide regulatory paperwork and oversight. The following protocols must be adhered to:

- An Form 2 ([http://www.selectagents.gov/resources/APHIS-CDC Form 2.pdf](http://www.selectagents.gov/resources/APHIS-CDC_Form_2.pdf)) must be filled out and submitted to ARO prior to transferring the agent. No select can be shipped unless the Form 2 is complete to be in compliance with Federal regulations.
- Recipient and shipper must have a registration number
- Shipper must receive confirmation in writing that shipment has been received. A copy of receipt will be sent to the RO/ARO.
- The RO/ARO of the recipient provides a completed paper copy or FAX of the Form 2 to the sender and to the HHS within 2 business days of receipt of the select agent or toxin.
- The recipient immediately reports to the HHS if the select agent or toxin has not been received within 48 hours after the expected delivery time or if the package received containing select agents or toxins has been leaking or was otherwise damaged.
- All shipments of biological agents will meet the packaging requirements defined by IATA "Shipping Infectious and Biological Substances."
- The quantity, volume or mass destroyed or otherwise disposed and the date of each action.
- Destruction/disposal of select agents requires specific documentation and submission of information to the RO or ARO. Please use the form found in Appendix A (http://www.ncsu.edu/ncsu/ehs/www99/left/bioSafe/forms/des_sel_agent.pdf) when agents are disposed or destroyed. Submit the form to the Biosafety Specialist for processing with the appropriate regulatory agency.
 - RO/ARO must be informed 7 days prior to destruction or disposal of select agent.
 - Destruction/disposal of select agents/toxins must adhere to State and Federal protocols.
 - Destruction must be witnessed by another individual.

Risk Assessment

Based on crime statistics provided by Campus Police and past occurrence of weather and fire events, the probability of occurrence and severity of impact has been evaluated for the following events:

| | | |
|--------------------|--------------------|-------------------|
| Freezer power loss | medium probability | high severity |
| Lab fire | low probability | high severity |
| Theft of agent | low probability | high severity |
| Hurricane damage | low probability | high severity |
| Tornado | low probability | high severity |
| Animal Activists | low probability | moderate severity |

The Physical Security Section of the plan will address cost effective strategies to protect critical facility assets where select agents are used.

Physical Security Systems

Based on the risk assessment the following precautions are required for select agent laboratories and recommended for other laboratories using biological agents or toxins:

- A graded level of security protection will be implemented based on site-specific risk and threat analysis
- Laboratories must be locked when unoccupied
- Keys or other security devices will be used to permit entry into these areas; key distribution must be controlled
- Lock all freezers, refrigerators, cabinets, incubators and other containers where select agents are stored when they are not in direct view of a laboratory worker
- Only authorized personnel will have access to select agents
- Unauthorized personnel entering select agent areas must be escorted and monitored by authorized personnel
- Visitor access to the area where select agents are used or stored must be controlled. A log will be kept with the following information:
 - The name of each visitor accessing area
 - Date and time of entry
 - Date and time of leaving
 - Access logs will be maintained by the lab personnel and made available to the RO/ARO and other authorized individuals.
 - An up-to-date list of persons who possesses door keys and knowledge of keypad access numbers or the security system.
- Personnel using select agents or toxins must report immediately the following to the RO.
 - Any loss or compromise of their keys, passwords, combinations

- Any suspicious persons or activities
- Any loss or theft of select agents or toxins
- Any release of select agents or toxins
- Any sign that inventory and use records of select agents or toxins have been altered or otherwise compromised.
- Routine cleaning, maintenance, repairs will only be done only when escorted and can be continually monitored by approved individuals.

Personnel Security and Reliability

Every new employee will be informed about the Biosecurity plan at new employee orientation. The training will provide information about restricted access areas, how they are identified and what unauthorized personnel must do to access these areas.

Unauthorized personnel entering into a restricted area will need to log in/out. All visitors will be escorted to the restricted area by an authorized employee and be required to log in/out.

Authorized personnel will not share their means of accessing the area where select agents or toxins are stored/used. This includes passwords, keys, keycards, or combinations.

The Biosafety Committee will not authorize the use of a select agent or toxin until the individual is approved by the HHS Secretary or the USDA Secretary based on a security risk assessment by the Attorney General.

- Each individual seeking clearance must submit a “Bioterrorism Preparedness and Response Act FBI Information” form FD-961 (<http://www.fbi.gov/terrorinfo/fd-961.pdf>) to the RO (RO/ARO will supply form upon request)
- The RO/ARO will submit the FD-961 to DOJ for processing.
- Individuals seeking clearance also will need to submit fingerprints to the FBI. Finger print cards will be sent to the RO after application has been processed.
- The following individuals are prohibited from accessing and using select agents or toxins as published by PHSBPRA
 - Is under indictment for a crime punishable by imprisonment for a term exceeding 1 year
 - Has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year
 - Is a fugitive from justice
 - Is an unlawful user of any controlled substance
 - Is an alien illegally or unlawfully in the U.S.?
 - Has been adjudicated as a mental defective or has been committed to any mental institution
 - Is an alien who is a national of a country as to which the Secretary of State has made a determination that such country has repeatedly provided support for acts of international terrorism –Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan

- Has been discharged from the Armed services of the U.S. under dishonorable conditions
- Has involvement with an organization that engages in domestic or international terrorism or with any other organization that engages in intentional crimes of violence
- Clearances will be valid for five years from date of approval.

Biosecurity Incident Response

Any security breach of a select agent use area must be immediately reported to the RO and Campus Police. By State Statute, Campus Police have jurisdiction over campus crimes. Any security breach will be investigated and prosecuted according to North Carolina State law.

Data, IT, and Cyber Security

- The greatest risk to information security is inadvertent disclosure by employees. The following measures will be taken to minimize these risks.
- *Hiring Permanent Employees*
Hiring supervisors are to review applications, carry out interviews and check references before making their final selection
(<http://www7.acs.ncsu.edu/hr/employment/>)
- *Work-Study Students and Temporary Employees*
Confidentiality and safeguarding of information should be covered by each work-study employer as students are hired to work in each department. Work-Study and other temporary employees shall have unique email addresses instead of sharing an address with past, present, or future temporary employees.
- *Existing Employees*
All current employees who have access to the select agent information must be informed of information security requirements.
- *Ongoing Training*
As part of the annual review process, the supervisor will review information security requirements with their respective employees or any employee who has access to select agent information.
- *Access to Select Agent Information*
Only employees whose job duties require them to access select agent information shall have access.

Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Lack of adequate procedures and technical controls creates a risk of unauthorized access to the information systems, and of accidental loss in the event of disasters or system failures. The following measures will be taken to minimize this risk.

- *Paper Storage Systems*
Supervisors should instruct employees on the need to keep confidential files out of public view, and also provide for storage of confidential files in locked cabinets wherever feasible.
- *Computer Information Systems*
The university has data ownership and access procedures that apply to all centrally managed data supported by administrative information systems under the jurisdiction of the Director of Administrative Computing Services. These procedures also apply to all user-developed systems that may access common University data.

The rules, procedures and guidelines govern the management and accessibility of central University data regardless of the environment where the data resides. This includes the central mainframe, departmental mini-computers, data servers, individual personal computers, and data as it resides in any other media (printouts, microfiche, etc.).

The Data Management Procedures may be found

at: <http://www.ncsu.edu/policies/informationtechnology/REG08.00.3.php>. Other documents applicable to security of computer information are the University-wide Computer Use regulation

(<http://www.ncsu.edu/policies/informationtechnology/REG08.00.2.php>)

- *Customer Information Disposal*
Administrative Computing Services erases all tapes and disks prior to disposal or surplus and adheres to the Department's procedure for cleaning storage medium.
- *Centralized Protection from E-Invasion*
The University's central administrative data is located behind a firewall and is protected in accordance with the Administrative Computing Services Data Network Procedures. Patches and maintenance for the systems in support of the administrative data are applied in accordance with the Administrative Computing Services System Maintenance Standards. The University has a site license for virus software, which is installed on applicable servers with central administrative data located in Administrative Computing Services.
- *Detecting, Preventing, and Responding to Security Breaches*
Prevention measures are addressed in prior sections. The risk to information security is compounded when breaches are not detected and remedied promptly. The following measures will be taken to minimize this risk. All information security breaches should be reported and rectified as soon as possible. Employees will be notified to report to their supervisors any suspected breaches of privacy or information security. The unit responsible for the information that has been compromised will report serious breaches to the Coordinators, who will keep a record of all such breaches and the remedies. Primary responsibility for detecting and remedying breaches lies with the supervisors in each unit. In addition, the Coordinators will look at the aggregate data for patterns among breaches to enable more preventive action. Employees and students who are at fault for breaches may be disciplined.