

# Generic Select Agent Biosecurity Plan Template

Generic text that may be appropriate to include in a facility's biosecurity plan is included below. Guidance on facility-specific information that should be included is provided in italicized text.

## 1 Introduction

*What is the goal of this plan? To whom does it apply? Indicate that it demonstrates compliance with specific federal regulations, such as 42 CFR 73, 9 CFR 121, or 7 CFR 331, and that it describes the full spectrum of measures taken to achieve graded protection of Select Agents (which should be defined in this introduction as a term used in this plan to refer to all CFR-regulated pathogens and toxins) against theft and sabotage. Indicate whether a single approach is being taken to secure all Select Agents at the facility or whether Moderate Risk and High Risk agents are being addressed separately (while still complying with all Federal regulations).*

## 2 Roles and Responsibilities

The roles and responsibilities included in this section are not all-inclusive but are intended to represent those functions related to implementation of the CFR requirements.

### 2.1 Responsible Official

The Responsible Official is an official authorized to ensure that the requirements of the CFRs are met. These requirements include developing and implementing this Biosecurity Plan. The Responsible Official (RO) will review this Plan annually and after any incident.

### 2.2 Alternate Responsible Official

The Alternate Responsible Official is an official authorized to act for the Responsible Official when the RO is unavailable.

### 2.3 Select Agent Supervisor

Select Agent Supervisors are individuals who are responsible for directing a project or program. Each Select Agent project or program is overseen by a Select Agent Supervisor, who is responsible for the scientific and technical direction of that project or program, and who has task authority over individuals who have permission to use Select Agents. Select Agent Supervisors are responsible for:

- ◆ Adopting the Biosecurity Plan procedures and ensuring that all personnel within their charge who have access to Select Agents familiarize themselves with the contents of the Plan and obtain biosecurity training annually
- ◆ Reporting Select Agent transfers, destruction, and inventory anomalies to the RO
- ◆ Requesting the RO to make Select Agent access authorization changes (See also Section 4.6.5)
- ◆ Providing the RO with any non-electronic visitor logs upon request
- ◆ Requesting changes to personnel access authorization
- ◆ Providing the RO with an up-to-date Select Agent registration packet.

### 2.4 Accountable Scientist

The accountable scientist, who may be a Select Agent Supervisor and/or a Principal Investigator, is responsible for Select Agent material control and accountability and Select Agent material transfers, as described in Sections 6 and 7.

## **2.5 Security Force**

*If a security force is employed, what is the nature of its responsibilities?*

## **2.6 Local Police**

*If applicable, what is the nature of the local police force responsibilities under a Memorandum of Understanding (MOU)?*

## **2.7 Specialty Personnel**

Specialty personnel may be employed by larger facilities. These may include Security Specialists who work in a Security Operations Center where an intrusion detection system is monitored, Physical Security Department Personnel, and Counterintelligence Personnel.

*Roles and responsibilities for these personnel should be spelled out in this portion of the security plan.*

## **2.8 Personnel Security**

The Personnel Security Division is responsible for initiating and monitoring necessary background screening and often, for evaluating the results.

## **2.9 Badge Office**

Badge Office Personnel are responsible for issuing and managing badges for regular and visiting personnel.

## **2.10 Information and Network Security**

Information and network security personnel include:

- ◆ The Chief Information Security Officer is responsible for network and information security policy for the facility; and
- ◆ The Center and Division Information Technology Officers are responsible for ensuring their respective network segments and information protection systems are implemented according to policy and that personnel are adequately trained on information and network security.
- ◆ System/Network Administrators are responsible for maintaining the system security, updating hardware and software, and responding to network intrusions.

## **2.11 Individuals with Select Agent Access Authorization**

In addition to other duties individuals have, individuals with Select Agent access authorization are responsible for:

- ◆ Protecting Select Agents while in their physical possession
- ◆ Protecting information related to Select Agents, while in their physical possession, in the context of verbal or electronic communication, and when storing it.
- ◆ Following all security-related procedures related to Select Agents, including those that apply to hosting and escorting procedures for visitors (See Sections 5.8 and 5.9)
- ◆ Reporting incidents and/or breaches in security to the appropriate Select Agent Supervisor and RO.

## 3 Basis for Biosecurity Program

### 3.1 Risk Assessment

This security plan reflects a risk management process in which assets and possible adversary actions (threats) are defined, and the resulting undesired events are evaluated based on their security risk. The risk assessment is an evaluation of the potential an adversary possesses to successfully execute an undesired event and the subsequent consequences. It establishes the set of risks a facility faces and presents them in ranked order so that the facility management may decide which risks will be protected against or mitigated and which risks will not. The security plan is based on this defined security risk posture, and demonstrates how the facility achieves protection and mitigation through a combination of security system design and incident response planning.

### 3.2 Graded Protection

Different assets require different levels of protection, accountability, and controls. The highest level of protection is given to the primary assets whose loss, theft, compromise, and/or unauthorized use will most seriously affect the national security, and/or the health and safety of employees, the public, the environment, or mission; e.g. High Risk pathogens. Slightly less protection is given to those secondary assets that may represent a Moderate Risk or that may assist an adversary in gaining access to, or diverting, a primary asset. Tertiary assets include operational assets and require somewhat less protection than the secondary assets. In this manner, the security system is designed to have graded levels, with the highest risk assets receiving the highest level of protection, and security increasing gradually as one moves physically closer to the asset.

*What types of assets would be considered Primary, Secondary and Tertiary at this facility?*

### 3.3 Assets

#### 3.3.1 Select Agents

Select Agents are those agents and toxins that have the potential to pose a severe threat to human, animal, or plant health, or to plant and animal products as defined by the CFRs.

*Which Select Agents does the facility possess?*

#### 3.3.2 Sensitive Information

Sensitive information is information that is too sensitive to be released to the public or to anyone who does not have an official purpose that requires him/her to hear, view, or have possession of the information (i.e., a need to know). Sensitive information is protected from unauthorized access and from disclosure under the Freedom of Information Act. See Section 8 for details on protecting sensitive information.

Sensitive information includes information related to the Select Agents, security-related information, and human resources information specific to those individuals who work with Select Agents.

##### 3.3.2.1 Select Agent Information

The following examples of sensitive information include, but are not limited to, the Select Agent records the Responsible Official is required to maintain:

- Select Agent information related to records described in the CFRs as:
  - A current list of all individuals with access to Select Agents;
  - Training records for individuals with access to Select Agents;

- Select Agent inventory records (including source and characterization data as well as any anomalies);
- Permits and transfer documents (CDC Form EA 101 and/or APHIS Form 2041);
- Visitor logs for laboratories containing Select Agents;
- Databases containing security and Select Agent information
- Documentation associated with experimental data or other data that has been restricted by the facility's review and approval process

### **3.3.2.2 Security Related Information**

The following examples of sensitive information include, but are not limited to, the security related records the Responsible Official is required to maintain:

- Security information related to the records described in the CFRs:
  - Security records (e.g., transactions from automated access control systems, testing and maintenance of security systems, visitor logs);
  - Containment and security incident reports;
  - Biosecurity Plan
- Details of facility description and blueprints especially as related to Limited and Exclusion Area designations and protection measures
- Details of vulnerabilities of those facilities that handle Select Agents and/or sensitive information
- Details of physical security (e.g., drawings and descriptions of security hardware and software systems)
- Details of computer systems and procedures
- Security procedures
- Badge design information
- Security system performance test results and audit results
- Incident reports and disciplinary actions
- Response force contracts and results of response force exercises

### **3.3.2.3 Human Resource Information**

Human resource information includes all information about personnel who work with or have access to Select Agents. This information includes:

- Home contact information
- Listings of family members
- Financial information
- Background investigation results

### **3.3.3 Critical Operational Assets**

Critical operational assets are those that may cause significant work delays or financial impact if destroyed or are directly involved in the security associated with High Risk Agents.

*Provide a list of the critical operational assets with a brief description of each.*

## **3.4 Threat Definition**

### **3.4.1 Insider**

The insider threat category includes a single, non-violent person with authorized access inside the facility. The insider is considered to be any person granted unescorted access to any portion of an Exclusion or Limited Area (see Sections 4.2 and 4.3 for further details on these areas). The intent of a malevolent insider is to steal, destroy, or release a

Moderate or High Risk agent, or to steal or destroy other high consequence assets at [facility name] without detection. The insider would be expected to abort any theft attempt to avoid identification. Authorized access affords this person extensive knowledge of the facility and operating systems. The insider has the opportunity to choose the best time to commit a malevolent act.

### **3.4.2 Outsider**

Outside adversaries can employ force, stealth, and deceit tactics to achieve their goals. Using force, the adversary makes no attempt to conceal acts or intention; the adversary simply overwhelms the system and personnel. Using stealth, the adversary attempts to enter the facility undetected to accomplish his goal. An adversary using deceit will attempt to accomplish his goal under the guise of authorized access through the use of forged credentials or other methods. Obviously, a sophisticated and well-trained adversary could employ a combination of all three tactics in order to steal, destroy, or release a defined asset. The outsider has access to only publicly available information and may be equipped with hand tools, may be armed, and may resort to violence (but is not suicidal).

## **3.5 Protection Strategy**

### **3.5.1 Insider Protection**

Traditional physical protection measures, personnel security programs, strict escorting rules, and material control and accountability procedures are the basic elements of the security strategy for protection against a malevolent insider. Of increased importance, given the difficulty with pathogen accountability, is the reliance that must be placed on employees and others with access to the pathogens. Stand-off detection technologies do not exist for biological agents, and inventory control systems will not necessarily reveal when material has been stolen or diverted. Thus, the insider threat is a daunting problem for biological research laboratories.

It is very difficult for a physical security system to prevent the theft or diversion of microorganisms by insiders. Therefore, it is paramount that biological research facilities do everything possible to ensure that those who have access to dangerous pathogens and toxins are reliable and trustworthy.

It should be noted that foreign nationals cannot be investigated as thoroughly as US citizens until the foreign national has resided in the US for the number of years that the investigation will cover. Until this point in time is reached, foreign nationals holding positions requiring a background investigation will represent a relatively greater risk than US citizens. Collusion is protected against in the same manner as any other insider threat.

### **3.5.2 Outsider Protection**

The strategy to protect against an outsider is to detect unauthorized access, through likely avenues of approach, to the biosafety containment labs or other areas where critical assets are located. Detection must be done in a timely manner and response forces summoned. These response forces may be private security forces or local law enforcement. When local law enforcement is employed, it is important to have a Memorandum of Understanding in place that outlines the conditions under which local law enforcement will respond, the response time that may be expected, and the protocol to follow once law enforcement arrives on site (due to possible biological containment issues).

The approach often used to achieve timely detection is to concentrate security upgrades at the physical locations where the pathogens or other critical assets are kept, and to control access to these locations.

## **4 Physical Security**

The physical security system limits access into defined security areas to authorized individuals with a valid need for access.

### **4.1 Property Protection Areas**

A Property Protection Area is defined by the outer-most perimeter of the facility. This security area is established to protect against damage, destruction, and theft of facility-owned property.

*What establishes the Property Protection Area (e.g. a perimeter fence)? What, if any, credentials are required to access the Property Protection Area?*

*What areas of the facility are Property Protection Areas? What assets are within this area?*

### **4.2 Limited Areas**

A Limited Area is a secured area, residing within the Property Protection Area, with barriers that identify its boundaries and encompass the designated space. The perimeter of a building often defines the boundaries of a Limited Area.

*What physical security measures are in place? What credentials are required to access the Limited Area?*

*What areas of the facility are Limited Areas? What assets are within this area?*

### **4.3 Exclusion Areas**

An Exclusion Area, like a Limited Area, is a security area with barriers that identify its boundaries and encompass the designated space, further restricting access beyond the Limited Area. Laboratories or storage areas that contain Select Agents are often designated as Exclusion Areas.

*What physical security measures are in place? What credentials are required to access the Exclusion Area?*

*What areas of the facility are Exclusion Areas? What assets are within this area?*

### **4.4 Long-Term Select Agent Storage**

*Are there differences in which area select agents can be stored if they are in locked storage containers (e.g. freezers, refrigerators)? If so, include the locations here.*

### **4.5 Security Operations**

#### **4.5.1 Access Hours**

*Does everyone have 24 hour access or do certain types of workers have access in different "time zones?" e.g. Mon-Fri, 6 a.m – 6 p.m; Mon-Sun. 6 a.m. – 6 p.m.; or 24 by 7.*

#### **4.5.2 Visitor Logs**

*In what rooms/areas are visitors required to sign log books? What information must be included? Does the escort also need to sign?*

#### **4.5.3 Vehicles**

*Who is authorized to park on site? Are there other parking restrictions, e.g. are private vehicles restricted from loading dock areas? Do personal cars require a parking sticker or placard? How is visitor parking handles?*

#### **4.5.4 Tailgating**

"Tailgating" is the practice of one individual following another into an area that has been restricted with an electronic security device (e.g. a proximity card) without utilizing his or her own means for unlocking the door. Tailgating is prohibited into any Limited or Exclusion Area. The term "tailgating" it is not used to describe the authorized entrance of individuals under escort, who follow additional escort/host procedures to insure accountability.

#### **4.5.5 Access Changes**

When an individual is re-assigned to an activity that does not require access to Select Agents, requires access to different Select Agents, or is initiating access to Select Agents, his/her access control authorizations must be updated. The Responsible Official reports any changes in Select Agent access to the CDC SAP/APHIS. The Responsible Official will immediately notify CDC SAP/APHIS when an individual's access to Select Agents is terminated; the Responsible Official must explain to CDC SAP/APHIS the reasons for terminating access. When an individual no longer needs access to a particular restricted area, these changes are also documented and electronic access devices are updated.

#### **4.5.6 Package Inspections**

*The CFRs require that all suspicious packages are inspected before they are brought into or removed from the area where select agents or toxins are used or stored.*

*Include under this section details regarding the specifics of suspicious package inspections: Is the inspection conducted in Shipping & Receiving? At the entrance of the laboratory? What are they inspected for? leaks, damage, etc? Who conducts package inspections?*

Employees should be suspicious of any mail that:

1. Is unexpected or from someone unfamiliar to you.
2. Is addressed to someone no longer with your organization or is otherwise outdated.
3. Has no return address, or has one that can't be verified as legitimate.
4. Is of unusual weight, given its size, or is lopsided or oddly shaped.
5. Is marked with restrictive endorsements, such as "Personal" or "Confidential."
6. Has protruding wires, strange odors, or stains.
7. Shows a city or state in the postmark that doesn't match the return address.

If you come in contact with any mail you consider suspicious, whenever you see an unattended or suspicious item on [the site name] properties, or if you receive a suspicious package, do handle the item. Call one of the numbers below.

[emergency hot line phone number] if the situation appears to be an emergency, or [non-emergency hot line phone number] if the situation appears to be a non-emergency. Please be prepared to provide the location and description of the suspicious package.

While waiting for emergency response personnel to arrive, please follow the guidance below:

1. Do not handle the parcel or contents further.
2. Isolate the parcel or contents and move personnel from the immediate area.
3. Ensure that everyone who has come into contact with the parcel or contents washes their hands thoroughly with soap and cold water.

## 5 Personnel Security

### 5.1 Position Risk Categories

#### 5.1.1 Low Risk

Low risk positions are positions that involve duties with the potential for limited impact on the agency or program mission or on the integrity and efficiency of the services provided.

##### 5.1.1.1 Background Investigation

*What types of personnel screening does the facility use for people in this category?*

##### 5.1.1.2 Job Categories

All [facility name] employees, contractors, and working visitors who do not fall into the Moderate or High Risk categories are considered to hold Low Risk positions. Personal and Casual Visitors are not given a risk designation.

*What types of job categories at the facility are considered low risk?*

#### 5.1.2 Moderate Risk

Moderate risk positions are those positions with duties that are of considerable importance to the agency mission, with significant program or delivery of service responsibilities. Moderate risk is the position risk level for the majority of positions associated with Select Agents.

##### 5.1.2.1 Background Investigations

*Moderate risk positions typically receive a more comprehensive background investigation than those in low risk positions. Sometimes, this is limited to the additional requirement of the DOJ Risk Assessment, if this category is limited to those who require access to Select Agents. These positions may also be subjected to a periodic reinvestigation.*

*What types of personnel screening does the facility use for people in this category?*

##### 5.1.2.2 Job Categories

*What types of job categories at the facility are considered low risk?*

#### 5.1.3 High Risk

High risk positions are those positions with duties that have a broad scope of responsibility and authority, which are especially critical to the agency or program mission.

##### 5.1.3.1 Background Investigations

*High risk positions typically receive a more comprehensive background investigation, and/or have a more restrictive authorization process. These positions may also be subjected to a periodic reinvestigation.*

*What types of personnel screening does the facility use for people in this category?*

##### 5.1.3.2 Job Categories

*What types of job categories at the facility are considered low risk?*

*If an employee has access to classified information, they are considered to hold a high risk positions. Generally, those positions at the top of the executive ladder and*

*those in high level positions of the security staff or IT staff who have access to the types of information that if released would make the facility vulnerable, are considered high risk.*

## **5.2 Reinvestigations**

The Responsible Official must request renewal of the CDC SAP/APHIS access approval every 5 years for as long as an individual needs access to Select Agents.

*What position risk categories, if any, have background investigations that will be routinely repeated on a periodic basis? What is the period between investigations?*

## **5.3 Access Limitations**

### **5.3.1 Employees**

Those individuals who require access to Select Agents must have CDC SAP/APHIS access authorization.

*Are there any other access limitations in place for limited or exclusion areas? E.g. must the background investigation be complete before an individual is allowed into an area without an escort? Must an individual meet any other requirements before being granted authorized access, e.g. yearly training? Immunizations?*

### **5.3.2 Visitors**

Visitors include personnel from universities, contractors, students, research fellows, visiting scientists, laboratory visitors, trades professionals, delivery personnel, etc. who, due to the duration of stay or nature of the work performed on site, are not provided with regular access to the facility. Visitors are escorted at all times in restricted (non-public) areas by an individual who has a complete and approved background investigation, access authorization, and a need-to-know. Visitors are expected to wear a visitor badge, sign all visitor logs, remain with their escort, and follow all facility policies and procedures, including the surrender of prohibited articles while on site.

Note: Facility/security managers may permit visitors to have unescorted access to restricted areas if the visitor is able to provide proof of an equivalent background investigation as that required of regular staff, including CDC SAP/APHIS authorization that has been processed by the facility's RO for access at the facility, if appropriate, and has legitimate business in these areas.

#### **5.3.2.1 Host Responsibilities**

Each visitor or group of visitors must have a host at the facility. The host must have a standard badge. The host is responsible for informing the visitor of the relevant policies and procedures, including access restrictions, prohibited articles, etc. The host may escort the visitor, or arrange for a separate escort who also has a standard badge and authorized escort into the areas to be visited.

*Include any department or individual that requires advance notice of expected visitor arrivals (e.g. Physical Security, receptionist, parking attendant, etc.), and what information is required (e.g. visitor name, arrival date and duration of stay).*

#### **5.3.2.2 Escorting**

An individual who has a standard badge and authorization to enter the areas to be visited must escort visitors.

*Are there different ratios of visitor to escort that apply in different areas, e.g. administrative offices vs. laboratories? Are visitors allowed on site only during certain hours? Are there certain areas where an escort is unnecessary?*

## **5.4 Foreign Nationals**

Foreign nationals from countries the US Secretary of State has determined to be supporters of international terrorism will not be approved for escorted or unescorted access into Select Agent areas.

## **5.5 Badging**

“Standard” badges will be issued to all employees and contractors. Visitors will be issued a distinct visitor badge. The name of the individual, name of facility, picture of the individual (for standard badges), and expiration date will be included on the badge.

*This section should accurately describe what features are included in the both the standard badge and the visitor badge, e.g. types of information, electronic access control (usually on standard badges), etc. This section should describe how long the badges are valid, e.g. 5 years for employees and contractors, or limited to the duration of stay for the visitor. It should describe any exceptions to wearing a badge (e.g. in laboratories, or under other conditions, where safety might be compromised). It should also describe the procedure an employee with a standard badge follows if his/her badge is forgotten, lost or stolen.*

# **6 Material Control and Accountability**

For the purposes of this section, “material” refers to repository stocks of Select Agents. Clinical samples and working stocks are not included.

## **6.1 Material Control**

All Select Agent materials are associated with specific laboratories, which are identified by campus (*if there are multiple campuses of the facility*), building number, floor, and room number. When materials are stored, the container (such as a freezer, refrigerator, or vault) is locked to restrict access.

Laboratory inventory is checked on an as-needed basis to confirm that records correspond to actual materials. Any discrepancies are reported to the RO. The inventory review may be initiated by the laboratory staff, or by request from the RO.

Any change to the association of a material with a laboratory is considered a material “transfer,” and is subject to the provisions of the Material Transfer Security section. Inventory records must be consistent with transfer operations.

Testing, diagnostic, and clinical samples are not controlled as part of the material inventory. Nevertheless, when isolates have been identified in clinical or diagnostic material as Select Agents, and those isolates are kept for future use, the isolates are added to material inventory as soon as they are stored.

Non-inventory samples that may contain Select Agent material must be destroyed as soon as they are no longer needed. When inventoried material is destroyed, however, the inventory record is updated accordingly—the record is not deleted.

## **6.2 Accountability**

Within each laboratory that uses or stores Select Agents, an accountable scientist maintains material inventory records, monitors the usage of materials, and oversees access to the materials. That accountable scientist is the contact person for the RO for any matters concerning the associated materials. The accountable scientist is usually a principal investigator or senior research scientist who normally works with the materials, and may be the Select Agent Supervisor, or someone designated by the Select Agent Supervisor. If a

laboratory works with more than one Select Agent, that laboratory may have separate accountable scientists for each agent. An accountable scientist may have a backup person, but otherwise the accountability is restricted to one individual. The accountable scientist ensures that the Select Agent Supervisor and Responsible Official are kept informed about changes to Select Agent inventories.

Other individuals within the same laboratory may have access to the areas where materials are stored and used, but the accountable scientist keeps the key to locked freezers or vaults where materials are stored. The accountable scientist may loan the key to others, but keeps a log of such usage. Others report what samples have been added or removed from storage so that the accountable scientist can keep the inventory records current.

### 6.3 Inventory Records

Each record of material inventory is kept in any one of a variety of forms, as determined by the accountable scientist. It may be in the form of an electronic database (such as MS Access or SQL Server), spreadsheet files (such as MS Excel), or handwritten in logbooks or card files. The inventory record may also serve a research purpose, and include additional information not required to meet the CFRs. Inventory records may also include non-Select Agent entries; but the Select Agent materials are identified as such to facilitate reporting. It is important that a single inventory be kept that satisfies both the biosecurity reporting requirements *and* any additional purpose.

Material inventory records are considered sensitive information, subject to the provisions of the Information Security section.

Each *record* in the material inventory refers to a distinguishable entity: either an individual item (such as a vial, ampoule, etc.) or collection of multiple items of the same Select Agent. If the latter, the record will further state the approximate quantity (such as mass, volume, number of items, etc.).

The information maintained about each inventory record (e.g., database *fields*) must include the following at a minimum, as required by 42 CFR 73.15 (b), and consistent with 7 CFR 331.14 (a) (4) and 9 CFR 121.15 (a) (4):

- Name and strain of the Select Agent
  - Source of the Select Agent:
    - How and when was the isolate acquired? Specific, private information about samples from human individuals is *not* required to meet 42 CFR 73 requirements, although it may be recorded for research purposes.
  - Location where stored:
    - The inventory record does *not* need to fully describe the location; for example, the rack / box / vial number may be specified explicitly, but the building / floor / room / freezer information may be the same for all, understood by the accountable scientist, and omitted from the record.
- Amount
  - Approximate values are sufficient
- Disposition
  - Date, recipient name, and approximate amount (for material transfer);
  - Date and approximate amount (for material destruction);
  - Explanation (for material lost, stolen, or otherwise unaccounted for)

42 CFR 73.15 (c) further mandates that a material *usage* log be kept for Select Agents. The material usage log may either be a separate table in a relational database, or usage could be recorded in a separate file. The usage information requires:

- Name and strain of the Select Agent
- Who used it
- When removed / when returned to storage
- For toxins only: quantity removed / quantity returned

## 6.4 Reporting

The accountable scientist maintains inventory records so that the records reflect the daily current status of actual Select Agent inventories and usage. A copy of the inventory record and/or usage log is provided to the RO when requested.

The accountable scientist is also responsible for immediately reporting any of the following situations to the RO:

- Material is missing (whether lost, stolen, or otherwise unaccounted for)
- Material has been released outside of the biocontainment area accidentally or otherwise
- Inventory discrepancies: the physical inventory does not match the book inventory
- Anomalies potentially affecting inventory (for example, if the key to a Select Agent freezer is missing)
- Any Select Agent samples, whether included in inventory or not, as soon as they are identified

The RO must immediately notify CDC or APHIS and appropriate Federal, State, or local law enforcement agencies.

## 7 Material Transfer Security

Material transfers require authorization through the RO and CDC SAP/APHIS prior to conducting external transfers. Materials transfers must also have transfer documentation and accountability maintained for Select Agents moving between Exclusion Areas during internal transfers.

Personnel background screening requirements for individuals who have access to Select Agents packages (e.g., shipping, receiving, and internal delivery) are in accordance with the Personnel Security Section.

### 7.1 External Transfers

External transfers consist of moving a Select Agent between a facility registered entity and an external, authorized entity. External transfers require secure movement within a facility prior to relinquishing custody to a commercial carrier or courier company.

External transfers follow authorization and documentation procedures outlined in 42 CFR 73, 9 CFR 121, and 7 CFR 331. Therefore, when sending Select Agents, the accountable scientist, in conjunction with the RO, ensures that:

- The sending and recipient RO possess the appropriate certificate of registration to cover the transfer, the transfer meets the exemption requirements found in 42 CFR 73.6 (a), or the agent is being transferred from outside the United States and all import permits/requirements have been met.
- The requesting facility has a certificate of registration specific to the Select Agent to be transferred.
- Prior to the transfer, the sender and RO for the recipient complete CDC Form EA-101 and/or APHIS Form 2041 and the sender submits the form to the proper agency for pre-transfer authorization.

When receiving Select Agent transfers, the facility accountable scientist, in conjunction with the RO, ensures that:

- The facility RO provides a completed paper or fax transmission of CDC Form EA 101 and/or APHIS Form 2041 to the sender and the CDC SAP and/or APHIS within two business days of receipt.
- Any damaged packages containing Select Agents are immediately reported to the receiving RO. The recipient must also immediately report to the receiving RO when a shipment has not been received within 48 hours of expected delivery time. In both cases, the RO must subsequently make an immediate report to the CDC SAP and/or APHIS as appropriate for the Select Agent involved.
- The recipient reports to the receiving RO, and the RO to the CDC SAP, within five days of material consumption or destruction in accordance with 42 CFR 73.21.

This facility also adheres to APHIS transfer permit requirements found under the organisms and vectors regulation 9 CFR 122 and plant pest regulation 7 CFR 330, as well as all Department of Commerce (DOC) export permit requirements found in 15 CFR Part 742, 744, and 774.

## **7.2 Shipping and Receiving**

This facility complies with all applicable transportation, shipping, packaging, and export laws related to Select Agents.

*Which personnel are responsible for ensuring compliance with all appropriate regulations? Are there any specific facility shipping or receiving procedures?*

## **7.3 Internal Transfers**

Internal Select Agent transfers occur as scientists and technicians exchange materials under study or add/remove Select Agents from the inventory through internal shipping and receiving processes. Any movement of Select Agent material into or out of a Select Agent-registered laboratory (i.e. all rooms managed by a single accountable scientist) is coordinated and authorized through the accountable scientist and must be documented in laboratory inventory records.

*Are there any specific forms or procedures (such as Chain of Custody forms) for transferring select agents between registered labs within the facility?*

# **8 Information and Network security**

## **8.1 Information Security**

### **8.1.1 Sensitive But Unclassified (SBU)**

Sensitive But Unclassified (SBU) is a designation that is applied by this facility to sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA) (5 U.S.C. 552). For information to be identified as SBU, it must fall within one or more of the FOIA exemption categories 2-9 (Exemption Category 1 is used for classified information).

Information related to Select Agents is generally unclassified, and if deemed sensitive, will be marked Sensitive But Unclassified (SBU).

*Some of the information related to Select Agents that may be deemed sensitive includes:*

- ◆ *Databases and lab records associated with Select Agents, including, but not limited to, inventory databases and chain of custody records*
- ◆ *Select Agent transfer records*
- ◆ *Documentation associated with an experiment resulting in an unexpected result banned by 9 CFR § 121.10*

*Security documentation, personnel and financial records are also often considered sensitive information.*

*Note: If sensitive information at the facility is categorized as something other than SBU, change text to reflect facility's marking requirements.*

### **8.1.2 Access to Sensitive Information**

No person will be authorized access to sensitive information unless that person has been determined to need to know that particular information in order to achieve an authorized purpose.

### **8.1.3 Protection of Sensitive Information While in Use**

Reasonable precautions will be taken to prevent access to sensitive information by persons who do not require the information to perform their jobs.

### **8.1.4 Communicating Sensitive Information**

Sensitive information may be communicated in the following ways:

- From person to person in direct contact with one another
- Over a land-line telephone
- Via first class, priority, or overnight mail, with no external markings that would indicate the material is sensitive
- Via fax machine when an authorized recipient is attending the machine
- By email to and from a facility email addresses ([...]*@facility*) that reside completely within the facility network (*if the network is deemed sufficiently secure by the Chief Information Security Officer or other qualified individual*) or when the information is encrypted.

### **8.1.5 Storage Rules for Sensitive Information**

All sensitive information existing in hard copy or removable electronic media should be stored within a locked container in a Property Protection Area or within a Limited or Exclusion Area, an access controlled electronic environment, or be under the physical control of an authorized individual. When Limited or Exclusion Areas are not available, for instance when an individual is traveling, a locked container within a locked room will suffice (e.g. locked briefcase or suitcase within a locked hotel room or vehicle).

### **8.1.6 Destruction of Sensitive Information**

Sensitive information will be destroyed by shredding or by any means available for classified information. Paper containing sensitive information will not be recycled.

Electronic or removable media will be physically damaged to the point of inoperability, via shredding, degaussing, melting, or other such methods before disposal.

### **8.1.7 Review and Approval Process**

Review and approval of any information to be released to the public, through the medium of a publication, conference presentation, press release, web site, or other form, will be conducted to ensure sensitive information is not inadvertently released.

*Specify who has the authority to approve the release of information.*

### **8.1.8 Operational Security (OPSEC)**

All personal identification numbers (PINs), passwords, badges, lock combinations, keys, and key locations, or other access-related knowledge or devices, are controlled by the individual who has been given authority to receive this information or device. These items are not shared with any other individual.

## **8.2 Network Security**

*How is the facility's network protected? What encryption technique is used for electronic information?*

### **8.2.1 Computer Processing**

The following rules are applied when processing SBU information on the computer:

- Computers processing SBU information are facility-owned and protected as a part of the overall network security program.
- Computers employ password-locking screen savers to protect information on the screen and to secure the computer when it is not attended.

## **9 Safety**

This facility follows the safety requirements as delineated for Biosafety Level 2, 3, and 4 laboratories, in accordance with the CDC/NIH publication *Biosafety in Microbiological and Biomedical Laboratories* (BMBL), fourth edition. Individual laboratories also develop and follow laboratory-specific safety manuals.

*If alternate or additional safety requirements, guidelines, or manuals are followed, they should be specified here.*

## **10 Emergencies and Security Incidents**

Emergencies and security incidents that must be reported to the Responsible Official include the following:

### **10.1 Loss or compromise of access control devices or information**

Access control devices and information include: keys, passwords, combinations, badges, card keys, smart cards, etc. that provide access to Select Agents or their storage, use, or transport areas. Loss or compromise of these items or information must be reported immediately to Security and the RO. Loss or compromise of other forms of sensitive information must also be reported immediately to Security.

### **10.2 Unauthorized persons**

All personnel with unescorted access to a Limited or Exclusion Areas must be familiar with how to determine whether other individuals in the area are authorized to be there. They are to approach any visitor or other person who appears not to be authorized, and/or observed to be conducting any suspicious activity in the area, as long as they appear non-threatening and challenge him/her by asking to see his/her badge. If the badge is a Visitor badge, and the individual is not under escort, the name of his/her escort and/or host must be obtained. If the individual or situation appears dangerous, or if the situation cannot be resolved, the authorized individual should contact the security manager immediately and leave the area. The Responsible Official must also be notified.

### **10.3 Loss, theft, or release of Select Agents**

The Responsible Official must be notified upon discovery of inventory suspected of being lost, stolen, or misplaced, and any inventory records suspected of being altered.

Upon notification, the Responsible Official will investigate and notify the appropriate Federal Agency, if necessary, by completing CDC Form 0.1316 or APHIS Form 2043 as appropriate.

*If the facility has spill response procedures, they should also be referenced here.*

### **10.4 Safety incidents involving Select Agents**

*Provide a reference to the appropriate facility response procedures.*

### **10.5 Emergency Management**

*Provide a reference to the appropriate facility emergency management plans.*

### **10.6 Suspicious packages in Exclusion Areas**

*Provide a reference to the appropriate facility incident response plan.*

## **11 Training**

*Provide details on the facility's training requirements (both safety and security). What will the training cover? Who must complete the training? How often is retraining required? What are the penalties for failure to complete the necessary training? How are training records maintained?*

## **12 Incidence Response Plan**

See Sections 73.14, 121.14, and 331.14 regarding incident response planning.

"The incident response plan must fully describe the entity's response procedures for the theft, loss, or release of a select agent or toxin, inventory discrepancies, security breaches (including information systems), severe weather and other natural disasters, workplace violence, bomb threats, suspicious packages, and emergencies such as fire, gas leak, explosion, power outage, etc. The response procedures must account for hazards associated with the select agent and toxin and appropriate actions to contain such select agent or toxin.

The incident response plan must also contain the following information:

4. The name and contact information (e.g., home and work) for the individual or entity (e.g., responsible official, alternate responsible official(s), biosafety officer, etc.),
5. The name and contact information for the building owner and/or manager, where applicable,
6. The name and contact information for tenant offices, where applicable,
7. The name and contact information for the physical security official for the building, where applicable,
8. Personnel roles and lines of authority and communication,
9. Planning and coordination with local emergency responders,
10. Procedures to be followed by employees performing rescue or medical duties,
11. Emergency medical treatment and first aid,
12. A list of personal protective and emergency equipment, and their locations,
13. Site security and control,
14. Procedures for emergency evacuation, including type of evacuation, exit route assignments, safe distances, and places of refuge, and
15. Decontamination procedures.

The plan must be reviewed annually and revised as necessary.

Drills or exercises must be conducted at least annually to test and evaluate the effectiveness of the plan. The plan must be reviewed and revised, as necessary, after any drill or exercise and after any incident.”