LABORATORY SECURITY POLICIES/PROCEDURES

I. GENERAL

These policies/procedures provide the necessary security requirements that must be followed in order to ensure the security and control of areas containing select agents and toxins and to safeguard the select agent or toxin against unauthorized access, theft, loss, or release.

Drills or exercises must be conducted at least annually to test and evaluate the effectiveness of the security plan. They must be documented to include how the drill or exercise tested and evaluated the plan, any problems that were identified and corrective action(s) taken, and the names of registered entity personnel participants. The plan must be reviewed and revised, as necessary, annually, after any drill or exercise and after any incident.

II. FACILITY SECURITY

A. A security guard is located at the main entrance to the building and patrols the interior and exterior areas at regular intervals. Security can be reached at (817) 321-4703.

B. Security personnel are on duty during the following hours:
6:00 am – 8:30 pm (Monday - Friday)

C. A surveillance camera is located in the hallway outside of room 1715 (the STD/Micro suite). This camera monitors entries and exits for rooms 1714 and 1715.

D. The laboratory facility is monitored by a security alarm system when no personnel are present.

III. PERSONNEL SECURITY

A. In order to obtain authorized access to select agents, all laboratory personnel requiring access to the area in which select agents are used or stored must undergo a criminal background check performed by the US Department of Justice. Authorized access will be granted once the check is complete and no restrictions have been detected. A list of restrictions may be found in 42 CFR Part 73, section 73.8.

B. All laboratory personnel approved for access to select agents must wear visible identification badges that include a photograph and the wearer’s name.

C. All laboratory personnel are trained and equipped to follow established procedures.
   1. Employees will receive training on security policies and procedures on an annual basis.
   2. New employees will receive security training immediately after hire.
   3. Training for all employees will be updated as policies and procedures change.
   4. All training will be documented by maintaining records of training schedules and employee attendance.

D. Pursuant to 18 USC section 175b, as added by section 817 of the US Patriot Act of 2001, P.L. 107-567, aliens (other than aliens lawfully admitted to the United States for permanent residence) are prohibited from possessing select agents if they are nationals of countries as to which the Secretary of State (pursuant to provisions of the Export Administration Act of 1979, the Foreign Assistance Act of 1981, or the Arms Export Control Act) has made an unrevoked determination that such countries have repeatedly provided support for acts of international terrorism.

IV. ACCESS CONTROL

A. Access to select agent areas must be limited to only authorized personnel who have been cleared by the US Department of Justice. A list of authorized personnel may be found in the Select Agent Inventory & Product Information manual.
   1. All visitors, maintenance workers, service workers, and others needing one-time or occasional entry must be escorted and monitored by authorized personnel.
      - Visitors must record each entry into and exit from the restricted areas in the appropriate visitor log, even if they plan to return the same day.
      - The authorized individual permitting visitor entry into a select agent area should escort the visitor for the duration of their time within the restricted space. The escort must also record their initials on the visitor log in the designated area.
      - If an escort must be relieved from their duties, the authorized escort assuming responsibility of the visitor should record their initials on the visitor log also.
      - Authorized personnel escorting visitors must maintain a line of sight with these individuals and must have no other duties while escorting. The restricted person is never allowed access to any select agent or toxin.
      - For all registered areas the restricted person will enter, all select agents and toxins will be secured against unauthorized access while the restricted person is in a registered area (e.g., select agents or toxins are removed from the area).

2. All visitors entering the laboratory must be issued visitor badges. Certain areas, such as rooms 1714 and 1714A (BSL-3 area) and 1715-1718 (STD/Micro suite) require additional security. Visitors must be escorted and monitored into and out of those areas. Visitor badges will only be issued for one entry at a time and returned before exiting the building. Visitors returning for multiple days must be issued a new badge each time access into the laboratory is required.
3. A visitor's log must be signed before entry into the laboratory is allowed. The necessary information to be obtained is date, time of arrival, visitor name and reason for visit, visitor badge issued, visitor badge number, escorted by, time of departure, and visitor badge returned.
4. An additional visitor's log must be signed before entry is allowed into the laboratory areas where select agents and toxins are stored or used. The necessary information to be obtained here is date, time of arrival, visitor name and reason for visit, if training was understood, escorted by, and time of departure.
5. Training must be accomplished prior to the individual's entry into areas where select agents or toxins are stored or used and documented on the appropriate log. The training for escorted personnel is based on the risk associated with accessing these areas. Training must occur annually, starting over at the beginning of each calendar year.
6. Routine cleaning, maintenance, and repairs must be limited to hours when authorized employees are present and able to serve as escorts and monitors.

B. Select agent areas must utilize methods of secure access.
   1. The doors into the main laboratory area are to remain locked at all times. Entry into the laboratory is attained by Chubb card access only.
      a. Upon arriving to work each day, a Chubb card must be used by all lab employees to gain entry into the lab. If the employee does not have their Chubb card, they must sign in on the Visitor Log upon arrival and departure.
      b. For BT section personnel requiring the use of their Chubb card for multiple entries into registered areas, if they forget their Chubb card at home, they must go back home and get it. Under NO circumstances will any individual share their unique means of accessing a select agent or toxin.
      c. Each entry into these areas must be recorded. Therefore, **each** person must swipe their Chubb card each time they enter. Gaining entry by following another SRA-approved individual inside is not allowed.
      d. A private, individual-specific PIN code is also required in addition to Chubb card access. All SRA-approved personnel must first swipe their Chubb card followed by entering their unique PIN

code. Both methods of access must be acceptable before entry is allowed.

e. For other laboratory SRA-approved personnel, if they forget their Chubb card at home and require access into the registered spaces on a limited basis, they must sign the Visitor's Log located outside those areas each time they enter.

2. The doors leading into rooms 1714 and 1714A (BSL-3 area) and 1715-1718 (STD/Micro suite) are to remain locked at all times. Select agents are stored in these areas. Entry into these areas is attained by Chubb card and PIN code access. Only DOJ approved personnel are granted Chubb cards exclusively activated to allow entry into these rooms and additional identification verification is done through unique PIN code authorization. *Note: Refer to Attachment A for laboratory floor plan indicating room number designations and locations.*
3. All select agents must be secured inside a lockbox/lock-drawer before placing into refrigerators or freezers for storage.
4. The distribution of keys/Chubb cards is controlled by the laboratory services division manager. A list of keys/Chubb cards and personnel who have authorized access to the keys/Chubb cards may be found in the *BT Select Agent Program Access Approvals, Select Agent Inventory & Completed Forms* manual.
5. Individuals with DOJ access approval must refrain from sharing with any other person their unique means of accessing a select agent or toxin (e.g., Chubb cards, punch key access codes, or PIN codes).
6. The loss or theft of keys, Chubb cards, punch key access codes, or PIN codes must be reported to the Responsible Official (RO) and section supervisor within one business day. Chubb card loss must then immediately be reported to the Tarrant County Facilities Office for inactivation of the Chubb card. Loss or theft of keys will require locks to be changed. Lost or compromised punch key access codes or PIN codes will require the codes to be changed. Building security will also be notified of any loss or theft of keys/Chubb cards or lost/compromised punch key access codes/PIN codes.
   a. If misplacement of keys or Chubb card is suspected, a thorough search must be made before the loss is reported.
   b. Chubb cards/ID badges must be kept separate from door keys and the door keys must be stored separately in a secure location.
7. Whenever employment with the laboratory is terminated by or for an employee, their Chubb card and PIN code access will be immediately inactivated. The codes for any punch key access in secure areas will be immediately changed.
8. Computer passwords or passwords to any secure website must not be shared with anyone. If those passwords are compromised, they must immediately be changed and the incident immediately reported to the Tarrant County Information Technology (IT) Division and/or the

Gatekeeper for those specific secure websites as well as to the Responsible Official.

9. Any loss of computers, hard drives or other data storage devices containing information that could be used to gain access to select agents or toxins must be immediately reported to the Tarrant County Information Technology (IT) Division as well as to the Responsible Official. The notification will facilitate notification of the Federal Bureau of Investigation (FBI) if deemed necessary by the Responsible Official as the loss of such equipment may be criminal in nature.
10. Unauthorized persons found in the select agent area will be immediately reported to the security guard on duty and removed from the premises. Any suspicious activity that may be criminal in nature will be immediately reported to the Responsible Official either in person or by cell phone and the appropriate law enforcement agencies notified. Those activities that may be considered criminal in nature include, but are not limited to, taking pictures of the laboratory without permission, loitering in areas around the laboratory with no purpose for being there, strange behavior, casing the area, and attempting to gain access into the laboratory.
11. A perimeter check of all laboratory doors must be done at the end of a regular business day. A log sheet must be filled out by the last person leaving the laboratory to verify that the check has been completed.
12. Any alteration of select agent inventory under false pretenses is strictly prohibited. If alterations are found, they must be immediately reported to the Responsible Official and the Alternate Responsible Official(s). Disciplinary measures will be determined by the Responsible Official at that time and any serious discrepancies will be reported to the appropriate agencies. If clerical errors are made while maintaining inventory records, the error should be crossed through with a single line, initialed and dated with the correction written legibly in ink.
13. Movement of BT personnel transporting select agents from registered areas through non-registered areas such as hallways/corridors will occur due to the design of the laboratory. When this is necessary, select agents are secured inside a sturdy hard plastic sealed container to prevent any accidental releases from occurring.
14. Permission is required from either the Responsible Official, Alternate Responsible Official(s), or Principal Investigator before work is allowed to be conducted on select agents and/or toxins after established work hours.

V. SELECT AGENT ACCOUNTABILITY

A. An inventory procedure has been established to ensure adequate control of select agents and maintain up-to-date inventory of agents in long-term storage.
   1. The select agent inventory records include name, characteristics, and data regarding the agent's location, use, storage method, source, and inventory (original vial lot number or case number, date received, quantity acquired from another entity, if stock cultures were made, number of stock culture

vials, stock culture lot number, initial volume of each vial, vial number used, date removed from storage, removed from storage by, date returned to storage, returned to storage by and date of final disposition/destruction).

2. The select agent inventory will also include a usage log. The information kept here will be original lot number, if stock cultures were made, number of stock culture vials, initial volume of each vial, stock culture lot number, vial number used, purpose of use, scrapings taken–number of plates inoculated, date inoculated, tech initials, number of plates destroyed, date of destruction, and tech initials performing destruction.
3. The data will be maintained in Microsoft Excel spreadsheets/log sheets and revised each time a select agent is accessed. The spreadsheets will be updated, signed and dated by the tech(s) utilizing the select agent. The spreadsheets will be maintained in a logbook that will be stored in a locked cabinet within a secured area.
4. Inventory will be reconciled on a monthly basis and recorded on the appropriate select agent inventory log sheet. Any agent(s) unaccounted for will be immediately reported to the Responsible Official and the Alternate Responsible Official(s). Once it is determined that the agent(s) are indeed lost, stolen, or released, the appropriate agencies will be notified. (See Section X.B. Incident Reporting.)
5. Any discrepancies discovered during an inventory check, such as typographical errors on the inventory sheets, typographical errors on the agent labels, or various other typographical-related errors or other inventory discrepancies not involving the loss, theft or release of any agents will be immediately reported to the Responsible Official and the Alternate Responsible Official(s). Corrections to that month's inventory sheet will be made with an explanation describing the discrepancy.
6. Handwritten records must be accurate and legible, have controlled access, and authenticity can be verified.
7. A complete inventory audit of all affected select agents and toxins in long-term storage must be conducted when any of the following occur:
    a. Physical relocation of a collection or inventory of select agents or toxins for those select agents or toxins in the collection or inventory.
    b. Upon the departure or arrival of a principal investigator for those select agents and toxins under the control of that principal investigator.
    c. In the event of a theft or loss of a select agent or toxin, all select agents and toxins under the control of that principal investigator.
8. All records must be maintained for three years.

VI. INFORMATION SYSTEMS CONTROL

A. The following statements describe the security for the Tarrant County Public Health's information system.

1. Tarrant County has a full time, experienced and certified Information Security Officer, Public Health HIPAA Security Officer, Public Health HIPAA Compliance Officer and Security teams.
2. Information Security is comprised of an OpSec Team that is responsible for day-to-day operational security and an ACI Team that manages **A**udit, **C**ompliance and **I**nvestigations.
3. The Tarrant County Public Health Compliance Officer manages the day-to-day Public Health HIPAA compliance including BAA's.
4. Information Security has a formal Information Security Program (ISP) that is Risk-Based aligning with HHS, NIST & CJIS. It includes the following components: Vision & Mission statement, Policies, Background Checks, Stringent Patch & Change Management, Network Perimeter Protection, Incident Management & Response, Auditing & Assessments, On/Off Boarding with "Least Privilege", Multi-Factor Authentication, Strong Encryption in transit and at rest, Enterprise-Level Firewalls and Intrusion Prevention Systems, Web and Email Filtering, Windows 10 Version 1909 or higher Operating System, Office 2016, Microsoft Defender Malware A/V which is "Always On" & "Always up-to-date", Disaster Recovery & Business Continuity Plans and finally, a multipronged attack or approach toward mandatory Security Awareness
5. In the event that access control systems or surveillance devices are rendered inoperable, back-up security measures are utilized, and storage back-up is done at the Tarrant County IT building downtown. There is a 90-day retention period for the Tarrant County network only.
6. Computer systems are internally networked, and internet access is through Tarrant County servers.
7. Tarrant County utilizes perimeter firewalls and intrusion systems are in place. These are monitored through the Tarrant County IT department.
8. Regular patching and updates are made to operating systems and individual applications by TCPH IT Operations Security (O/S). They are checked every 30 days. Regular patching, system updates and software updates are performed as necessary.
9. Only authorized and authenticated users are granted access to select agent and toxin related information, files, shared folders, equipment and applications as necessary to fulfill their roles and responsibilities. Access is restricted and protected by passwords. The system requires a password change every 45 days and passwords cannot be reused.
10. Anti-virus software is used for the network and servers. Controls are in place that are designed to prevent malicious code (such as, but not limited to, computer virus, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to registered spaces. Anti-virus software provides these controls and aids in preventing cyber attacks.
11. There are some restrictions in place regarding internet browsing. Examples of those restrictions are sites containing pornography and using key letter flags on websites. Other restrictions can be added and users can be monitored.

12. The e-mail servers are protected by a restricted download policy. This is done by file extension and by file size.
10. Any breaches in information security would be immediately reported to the Responsible Official, Alternate Responsible Official(s) and to Tarrant County IT Operations Security (O/S). The laboratory would then follow all instructions from O/S. After completing an assessment of the scope and severity of an incident, the Responsible Official and Alternate Responsible Official(s), in conjunction with the IT Operations/Security Office will determine the appropriate next steps and make the required notifications, if needed. The Information Security Officer for Tarrant County should be contacted for any IT security-related concerns.

VII. RESPONSIBLE OFFICIAL

A. As a condition of conducting activities regarding select agents, an individual must be identified and authorized as the Responsible Official (RO). That individual must be approved by the HHS Secretary or Administrator following a security risk assessment by the Attorney General. He/she must be familiar with the requirements of this part, have the authority and responsibility to act on behalf of the entity, and ensure compliance with the requirements of this part. The Responsible Official for this facility has been identified as the Laboratory Division Manager.

B. The Responsible Official may identify one or more individuals, any of whom may serve as the Alternate Responsible Official when the Responsible Official is unavailable. These individuals must have the authority and control to ensure compliance with the regulations when acting as the Responsible Official. The Alternate Responsible Officials for this facility have been identified as the Laboratory Response Coordinator and the BT Section Supervisor.

C. The Responsible Official is responsible for ensuring compliance with the regulations. The Responsible Official must:
   1. Develop and implement biosafety, security and incident response plans.
   2. Allow only approved individuals access to select agents.
      a. Maintain an up-to-date, accurate list of the individuals approved for access to select agents.
   3. Provide appropriate training for biosafety, security and incident response.
   4. Transfer select agents in accordance with regulations.
   5. Provide timely notice of any theft, loss, or release of a select agent or toxin.
   6. Maintain detailed records of information necessary to give a complete accounting of all activities related to select agents.
      a. Maintain an accurate, current inventory of each select biological agent held.
      b. Maintain records documenting employee access to areas where agents are used or stored and the removal of agents from storage.

c. Implement a system to ensure that all records are accurate, and authenticity of the records may be verified.
d. Create records concerning inspections conducted.
e. Maintain records created for 3 years.

7. Have a physical (and not merely a telephonic or audio/visual) presence at the registered entity to ensure that the entity is in compliance with the select agent regulations and be able to respond in a timely manner to onsite incidents involving select agents and toxins in accordance with the entity's incident response plan.
8. Report the identification and final disposition of any select agent or toxin contained in a specimen presented for diagnosis or verification.
9. Immediately report by telephone, facsimile, or e-mail the identification of any of the following select agents or toxins: *Bacillus anthracis, Bacillus cereus* Biovar *anthracis,* Botulinum neurotoxins, Botulinum neurotoxin producing species of *Clostridium, Burkholderia mallei, Burkholderia pseudomallei, Francisella tularensis,* Ebola viruses, Marburg virus, Variola major virus (Smallpox virus), Variola minor (Alastrim), or *Yersinia pestis.* The final disposition of the agent or toxin must be reported by submission of APHIS/CDC Form 4 within seven calendar days after identification. A copy of the completed form must be maintained for three years. These documents will be maintained in the Electronic Federal Select Agent Program (eFSAP) Information System.
10. To report the identification and final disposition of any other select agent or toxin, APHIS/CDC Form 4 must be submitted within seven calendar days after identification. A copy of the completed form must be maintained for three years. These documents will be maintained in the Electronic Federal Select Agent Program (eFSAP) Information System.
11. Less stringent reporting may be required based on extraordinary circumstances, such as a widespread outbreak.
12. Report the identification and final disposition of any select agent or toxin contained in a specimen presented for proficiency testing. To report the identification and final disposition of a select agent or toxin, APHIS/CDC Form 4 must be submitted within 90 calendar days of receipt of the agent or toxin. A copy of the completed form must be maintained for three years. These documents will be maintained in the Electronic Federal Select Agent Program (eFSAP) Information System.
13. Conduct annual inspections of each registered space where select agents are stored or used to ensure compliance with all of the procedures and protocols of the biosafety plan. The results of these inspections must be documented, and any deficiencies identified during inspections must be corrected and the corrections documented.
14. The security plan must be reviewed by the RO at least annually and after any incident.
15. Immediately notify CDC or APHIS when an individual’s access to select agents or toxins is terminated by the entity and the reasons therefore.

16. Ensure that individuals are provided the contact information for the HHS Office of Inspector General Hotline and the USDA Office of Inspector General Hotline so that they may anonymously report any biosafety or security concerns related to select agents and toxins.

    OIG Hotline Contact Information
    Voice: 1-800-HHS-TIPS (800-447-8477)
    Fax: 1-800-223-8164
    Web: https://oig.hhs.gov/fraud/report-fraud/index.aspexternal icon
    Mail:
    Office of Inspector General
    Department of Health & Human Services
    Attn: Hotline
    P.O. Box 23489
    Washington, DC 20026

    USDA OIG Hotline Contact Information
    Voice: 1-800-424-9121
    Fax: 1-202-690-2474
    Mail:
    United States Department of Agriculture
    Office of Inspector General
    P.O. Box 23399
    Washington, DC 20026-3399

17. For visiting FSAP-approved persons, a Responsible Official (RO) must immediately notify the RO of the visited entity if the person's access to select agents and toxins has been terminated.
18. Immediately notify CDC or APHIS when an individual's access to select agents or toxins is terminated by the entity and the reasons therefore.
19. Investigate to determine the reason for any failure of a validated inactivation procedure or any failure to remove viable select agent from material. If the Responsible Official is unable to determine the cause of a deviation from a validated inactivation procedure or a viable select agent removal method; or receives a report of any inactivation failure after the movement of material to another location, the Responsible Official must report immediately by telephone or email the inactivation or viable agent removal method failure to CDC or APHIS.
20. Review, and revise as necessary, each of the entity's validated inactivation procedures or viable select agent removal methods. The review must be conducted annually or after any change in Principal Investigator, change in the validated inactivation procedure or viable select agent removal method, or failure of the validated inactivation procedure or viable select agent removal method. The review must be documented, and training must be conducted if there are any changes to the validated inactivation procedure, viable select agent removal method, or viability testing protocol.

VIII. RECEIVING SELECT AGENTS

A. A visual inspection of all packages is required upon entry to and exit from the receiving area.

B. Suspicious packages should be quarantined, and the Federal Bureau of Investigation (FBI) notified.

C. When opening packages containing specimens, bacterial, or virus isolates, a containment device such as a biological safety cabinet must be used.

D. Packages should only be opened by trained, authorized personnel.

E. If any packages containing select agents are delivered to the Customer Service desk or Central Supply, these packages will be treated the same as any other package where that package will be delivered to the person it is addressed to in the laboratory. This method is in compliance with the "lost in the crowd" concept and will maintain select agent anonymity during the shipping and receiving process.

F. Unexpected or unscheduled shipments of packages containing potentially infectious materials could possibly arrive from Sentinel (hospital) laboratories and will be labeled as either "UN 3373 Biological Substance, Category B", or "UN 2814 Infectious Substance, affecting humans". If a package should arrive before or after business hours (8:00 am to 5:00 pm), the Customer Service desk/security guard will notify laboratory administrative staff that a package has arrived and will hold the package until it can be received by laboratory personnel. This process would be followed for any package labeled as either "UN 3373 Biological Substance, Category B", or "UN 2814 Infectious Substance, affecting humans". These packages may require refrigeration/freezing and should not be left at the Customer Service desk or in Central Supply. The Federal Select Agent Program should be notified of all unexpected select agent and toxin shipments immediately (within 24 hours of receipt).

G. If a package containing select agents or toxins has not been received within 48 hours after the expected delivery time or has been damaged to the extent that a release of a select agent may have occurred, the recipient must immediately report this incident to FSAP. In addition to the initial reporting, the entity must follow up with a written report (*APHIS/CDC Form 3* – Incident Notification and Reporting (Theft, Loss or Release)) within 7 calendar days of the incident.

H. For additional information regarding the shipment of select agents, please refer to the *Procedure for Receipt of Packages Containing Potentially Infectious Materials* and *Policy for Biological/Chemical/Radiological Specimens for*

Submission, Transport, Transfer, and Handling found in the *Bioterrorism Section Laboratory Operations Procedures/Policies* manual.

IX. TRANSFER OR SHIPPING OF SELECT AGENTS

A. To obtain authorization for transfer, *APHIS/CDC Form 2 – Request to Transfer Select Agents and Toxins* must be submitted. This form may be found on CDC's website at http://www.selectagents.gov using the forms tab located near the top of the page.

B. Select agents that are to be transported are to be packaged and labeled in conformance with all applicable local, federal, and international transportation and shipping regulations, including:
   1. U.S. Department of Transportation - 49 CFR 171-180, U.S. Department of Transportation Hazardous Materials Regulations
   2. United States Postal Service - 39 CFR Part 20, International Postal Service (International Mail Manual) and Part 111, General Information on Postal Service (Domestic Mail Manual)
   3. Technical Instructions for the Safe Transport of Dangerous Goods by Air (Technical Instructions) – International Civil Aviation Organization (ICAO)
   4. Dangerous Goods Regulations – International Air Transport Association (IATA)
      a. Verify carriers have an en-route security plan for hazardous materials transported on behalf of Tarrant County Public Health.
      b. Verify carriers used comply with all applicable regulations, federal and state laws that apply to the services offered.
      c. Work with any future carriers to determine a security plan in the event that no plan has been identified.
      Note: Carriers need not provide copies of internal policies and procedures.

C. USA Couriers, Inc. has been selected as the carrier of choice by Tarrant County for the shipment of Category A Infectious Substances. Their security plan provides USA Couriers, Inc with a security and emergency preparedness capability that will:
   1. Meet any applicable Federal security requirements.
   2. Ensure that security and emergency preparedness are addressed during all phases of their operations.
   3. Promote procedures and practices that will ensure secure operations are maintained through the on-going identification, evaluation and resolution of security threats and vulnerabilities.
   4. Create a culture that supports personal security and safety and secures their operations (during normal and emergency conditions) through compliance with company rules and procedures.

5. Achieve a level of security performance and emergency readiness that meets or exceeds the operating experience of similarly sized companies around the nation, but primarily promotes general health and wellbeing to our communities.

Note: Packaging and shipping procedures may be found in the Bioterrorism Section Laboratory Operations Procedures/Policies manual.

D. Decontaminate contaminated or possibly contaminated materials before they leave the laboratory area.

E. If select agents are to be hand-carried on common carriers, all applicable packaging, transport, and training regulations should be followed.

F. Packaging of select agents for shipment may only be performed by individuals approved by the HHS Secretary or Administrator to have access to select agents and toxins and is in compliance with all applicable laws concerning packaging.

G. Intra-entity transfers do not occur at this facility. The laboratory's location at 1101 S. Main Street, Fort Worth, TX, 76104, is the only facility covered under the existing certificate of registration.

H. If any packages containing select agents are to be shipped, these packages will be treated the same as any other package, whereas that package is prepared according to the "lost in the crowd" concept and will be taken to the laboratory front desk where it is to be picked up by a courier. This practice will maintain select agent anonymity during the shipping and receiving process.

X. INCIDENT REPORTING

A. Unauthorized persons found in the restricted select agent area will be immediately reported to the security guard on duty and removed from the premises. Any suspicious activity that may be criminal in nature will be reported to the Responsible Official and appropriate law enforcement agencies. The Responsible Official will immediately notify the Federal Bureau of Investigation (FBI) of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins.

B. Inventory shall be reconciled on a monthly basis and recorded on the appropriate log sheet(s). If any select agents or toxins are unaccounted for during inventory or at any other time and discovered by an individual with access approval from the HHS Secretary or Administrator, that individual will immediately report their findings to the Responsible Official and Alternate Responsible Official(s). Once it is determined that the agent(s) are indeed lost, stolen, released, or misused, the appropriate agencies will be notified. The Texas Department of State Health Services (DSHS) shall be notified, as well as the Centers for Disease Control and Prevention (CDC), the Department of Health and Human Services (DHHS) and/or

the United States Department of Agriculture (USDA). The notification must be reported to the HHS Secretary by either telephone, facsimile, or e-mail in accordance with 42 CFR Part 73.21. The Centers for Disease Control and Prevention (CDC) Select Agent Program must be notified using *APHIS/CDC Form 3* – Incident Notification and Reporting (Theft, Loss or Release). This form may be found on CDC's website at http://www.selectagents.gov using the forms tab located near the top of the page. The appropriate law enforcement agencies will be notified pending direction from CDC.

C. A release is considered a discharge of a select agent or toxin outside the primary containment barrier due to a failure in the containment system, an accidental spill, occupational exposure, or a theft. Any incident that results in the activation of a post exposure medical surveillance/prophylaxis protocol will be reported as a release. Any release will be immediately reported to the Responsible Official and Alternate Responsible Official(s). The Centers for Disease Control and Prevention (CDC) Select Agent Program must be notified using *APHIS/CDC Form 3* – Incident Notification and Reporting (Theft, Loss or Release). This form may be found on CDC's website at http://www.selectagents.gov using the forms tab located near the top of the page.

D. Any incident(s) involving select agent occupational exposure or breaches of primary containment will be immediately reported to the Responsible Official and Alternate Responsible Official(s). The incident(s) will also be reported to the Texas Department of State Health Services (DSHS).

E. Any breaches in security measures will be immediately reported to the Responsible Official and Alternate Responsible Official(s). Decisions will be made at that time as to whether law enforcement agencies will be notified depending on the severity and type of the security breach.

XI. REFERENCES

A. *Federal Register*, Department of Health and Human Services, Part III, Volume 70; 42 CFR Part 73; 7 CFR Part 331; 9 CFR Part 121; March 18, 2005

B. *Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents*, Centers for Disease Control and Prevention (CDC), Office of Health and Safety, *Biosafety in Microbiological and Biomedical Laboratories (BMBL)*, 4th Edition, Appendix F, December 5, 2002

C. *Biosafety in Microbiological and Biomedical Laboratories (BMBL)*, 5th Edition, Section 6, U.S Department of Health and Human Services, Centers for Disease Control and Prevention & National Institutes of Health; February 2007

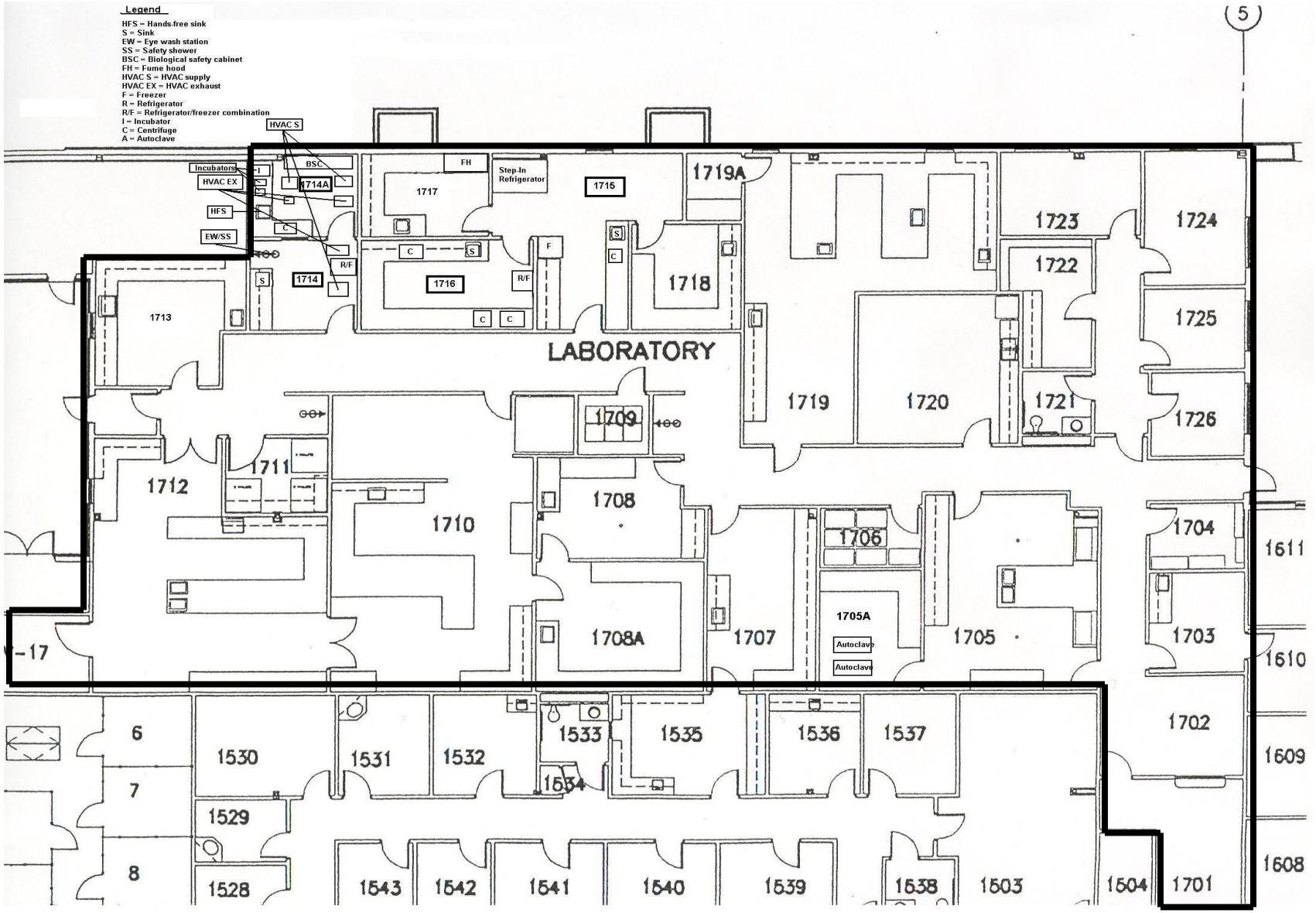
D. *Select Agents and Toxins Security Information Document*, 7 CFR Part 331.11, 9 CFR Part 121.11, 42 CFR Part 73.11; U.S. Department of Health and Human

Services, Centers for Disease Control and Prevention, Division of Select Agents and Toxins; U.S. Department of Agriculture, Animal and Plant Health Inspections Service (APHIS), Agriculture Select Agent Program; March 8, 2007

E. *Inspection Checklist for Security,* 7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73; U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, Division of Select Agents and Toxins; U.S. Department of Agriculture, Animal and Plant Health Inspections Service (APHIS), Agriculture Select Agent Program; April 4, 2013

F. *Guidance on the Transfer of Select Agents and Toxins*, Centers for Disease Control and Prevention, Division of Select Agents and Toxins

Attachment A – Laboratory Floor Plan



Revised date: 6/23/2025
Revised by: Erin Taylor