**Loss or Compromise of Keys, Passwords, Combinations, Access Cards, or Access Codes SOP**

INSTRUCTIONS: The below document is identified as a draft to be customized in consultation with INSTITUTION NAME personnel to ensure it accurately describes site procedures and requirements.

* **Black text** can be considered generic text that may be appropriate for inclusion.
* ***Red text*** should be considered guidance or examples and must be reviewed and replaced with facility-specific information.

1. **Scope**

This document applies to all personnel at the INSTITUTION NAME.

1. **Purpose**

The purpose of this SOP is to describe procedures in the case of a loss or compromise of keys, passwords, combinations, access cards, or access codes.

1. **Principle**

The loss or compromise of keys, access cards, access codes, passwords, or combinations for any area but especially for restricted or biological restricted areas, whether by unintentional actions, adversarial action, or staff changes, represents a fundamental compromise of the security at INSTITUTION NAME. In the event of such an event, immediate action must be taken to restore the security of the compromised area.

1. **Responsibility** 
   1. It is the responsibility of all personnel to maintain the integrity of all keys, passwords, combinations, access cards, and access codes they are issued and to immediately follow the procedures described in this document in the event of a compromise.
2. **Definition and Abbreviations**

**Access Control System:** An electronic system consisting of software and hardware that is networked to a site’s electronic access control devices (e.g., electric locks, card readers). The system integrates advanced security technologies and networking capabilities to provide a centralized monitoring and management system for a site’s electronic access control points.

**Alternate Responsible Official:** The person with authority and responsibility to ensure security requirements for restricted and biological restricted areas are met in the absence of the RO.

**Assistant Biological Safety Officer (ABSO):** The person who is responsible for identification and management of biological safety in particular, and biological risks in general, throughout the INSTITUTION NAME, in liaison with other members of the Biorisk Management Committee, Department Heads, and the staff of the INSTITUTION NAME in the absence of the BSO.

**Biological Restricted Area:** Biological Safety Level (BSL) 2 and 3 laboratories and any areas containing identified Especially Dangerous Pathogens (EDPs) and Valuable Biological Materials (VBMs) or areas where access to EDPs/VBMs is possible. Entry will be subject to special access restrictions. Physical security controls will be used to control access and secure property and materials. Biological Restricted Areas may be of different types depending on the nature and varying degree of access to EDPs/VBMs, or other relevant matter contained in the area.

**Biological Safety Officer (BSO):** The individual responsible for the identification and management of biological safety in particular, and biological risks in general, throughout the INSTITUTION NAME, in liaison with other members of the Biorisk Management Committee, Department Heads, and the staff of the INSTITUTION NAME. The BSO is the senior RO for all matters related to safety and biological safety at INSTITUTION NAME.

**Central Alarm Station (CAS)/Secondary Alarm Station (SAS):** Physical locations that provide centralized monitoring capability for all security layers throughout a site.

**Certifying Official(s)**: The person (or committee of people) responsible for certifying personnel for access to Restricted and Biological Restricted Areas.

**Closed-Circuit Television (CCTV):** The use of video cameras to transmit a video signal to a specific place, on a limited set of monitors, also known as video surveillance. It is a means of remotely monitoring specific locations.

**Deputy Security Manager:** A full-time employee (FTE), the Deputy Security Manager Is responsible for assisting the Security Manager in managing the security operations for INSTITUTION NAME. In addition, in the absence of the Security Manager or when the Security Manager must fulfill other, exclusive functions (e.g., Incident Commander), the Deputy Security Manager is responsible for the day-to-day security of INSTITUTION NAME, its personal assets, equipment, materials, cultures, specimens, and the protection of the public and the environment as related to security and biological security at INSTITUTION NAME.

**Especially Dangerous Pathogen (EDP)**: Those pathogens on the United States Select Agents List and others that may be determined by the (enter governing body here), or other governing body, to have the potential to pose a severe threat to the public, animal or plant health, or to animal or plant products.

**Incident Commander:** The person with overall responsibility for all aspects of an emergency response, including quickly developing incident objectives, managing all incident operations, application of resources as well as responsibility for all persons involved.

**Information Technology Manager:** Manages the application of computers, computer networks, and other information distribution technologies (including but not limited to television and telephone technology) to store, study, retrieve, transmit, and manipulate data or information at INSTITUTION NAME.

**Personnel Reliability Plan:** The plan to ensure that each individual who is authorized to access EDPs, and to escort and/or supervise personnel with access to Biological Restricted Areas and EDPs, including BSO/ABSO, Security Managers, Responsible and Certifying Officials, meet the highest standards of integrity, trust, personal reliability, and accountability so as to ensure these individuals do not pose a risk to the public health and safety, the environment or national security.

**Responsible Official (RO):** An individual, as designated by the Director of INSTITUTION NAME, who has the authority and responsibility to ensure security requirements for restricted and biological restricted areas are met.

**Restricted Area:** An area designated by the Director of INSTITUTION NAME (or by request of the Responsible Official (RO), Security Manager, or BSO) that houses valuable, sensitive, or hazardous material and requires access control.

**Security Manager:** A full-time employee (FTE), the Security Manager is responsible for the day-to-day security of INSTITUTION NAME, its personal assets, equipment, materials, cultures, specimens, and the protection of the public and the environment as related to security and biological security at INSTITUTION NAME. The Security Manager is the senior RO for all matters related to the security and biosecurity at INSTITUTION NAME.

**Valuable Biological Materials (VBMs)**: Biological materials that require (according to their owners, users, custodians, caretakers, or regulators) administrative oversight, control, accountability, and specific protective and monitoring measures in laboratories to protect their economic and historical (archival) value, and/or the population from their potential to cause harm. VBM may include pathogens and toxins, as well as non-pathogenic organisms, vaccine strains, foods, genetically modified organisms (GMOs), cell components, genetic elements, and extraterrestrial samples.

1. **Reagents:**

Not applicable

1. **Materials:**

Not applicable

1. **Related Directives**

INSTITUTION NAME Security and Biosecurity Plan

INSTITUTION NAME Personnel Reliability Plan

INSTITUTION NAME Job Description - Security Manager

INSTITUTION NAME Job Description – Deputy Security Manager

INSTITUTION NAME Job Description – Certifying Official

INSTITUTION NAME Job Description – Incident Commander

INSTITUTION NAME Job Description – Biological Safety Officer

INSTITUTION NAME Job Description – Assistant Biological Safety Officer

### Procedure

* 1. At least annually, an "in-use" audit will be conducted for all access control keys and cards to determine if there has been a loss or functionality issues.
  2. Upon loss or compromise of keys, access cards, access codes, passwords, and combinations, etc., or upon staff changes at INSTITUTION NAME in general, and particular, with respect to the access to, control, and securing restricted areas or biological restricted areas or any other access to Extremely Dangerous Pathogens (EDPs):
     1. Access controlled by electronic means (including access codes, computer passwords, and combinations) is to be changed **immediately**.
     2. Access to with protections that include the use of a standard lock and key will have the locks replaced **immediately**, including the purchase or replacement of the lockboxes, if appropriate.
  3. Any keys lost or compromised by INSTITUTION NAME personnel shall be reported to the Security Manager, BSO, and RO **immediately**, who shall decide whether the associated door, storage or locking container (if not attached to a restricted or biological restricted area), is critical enough to warrant changing the physical locks.
  4. The loss of a key shall also be recorded as such in the appropriate key control logbook. Access cards that are lost shall be reported immediately to the Security Manager, BSO, and RO, who shall promptly dis-enroll that card within the access control system and issue a replacement card, as appropriate.
  5. Additionally, the Security Manager will communicate the loss of the card immediately to appropriate management personnel, and if determined necessary, conduct follow-up, and an investigation will be initiated to determine and to prevent any unauthorized use of the access credential.
  6. The Security Manager, in coordination with the BSO, RO, and IT Manager must also ensure that all password-protected computer-based systems used for biosecurity (e.g., access control system, CCTV, central and secondary alarm stations, Pathogen Asset Tracking System [PACS]) are provided with strong passwords that are changed on a regular basis, as well as ensuring the systems are kept up-to-date with all IT security measures (e.g., anti-virus, anti-malware, software patches).
  7. The Security Manager, BSO, and RO are responsible for educating all staff members regarding how to properly protect their access cards, access codes, keys, user passwords, and the basic security provisions thereof.
  8. The Security Manager shall lead an investigation into the loss or compromise of all keys, passwords, access codes, and/or access cards to determine the root cause and recommend any improvements to the Biosecurity Plan to prevent future occurrence and recommend disciplinary action if and as appropriate based on HR (Human Resources) policies.
  9. An inventory of EDPs will be conducted prior to the issuance of new access privileges, access cards, access codes, combinations, and keys to new or reassigned Personal Reliability Program (PRP)-approved individuals.

# Safety Instructions

# Comply with all INSTITUTION NAME safety policy, while following the procedures described in this document.

# Reference

* INSTITUTION NAME Security & Biosecurity Plan
* INSTITUTION NAME Personnel Reliability Plan
* World Health Organization Biorisk management Laboratory biosecurity guidance, September 2006.
* European Committee for Standardization, Comité Europé De Normalisation (CEN) Europäisches Komitee Fűr Normung, Workshop Agreement (CWA) 15793
* United States Federal Select Agent Program