EDUCATIONAL INSTITUTION / NON-PROFIT ORGANIZATION
INDIVIDUAL SECURITY PLAN

Subcontractor Name: _____________________________________________

Subcontract Worker: ____________________________________________

Worker’s Full Name

P.R. / Subcontract #: _____________________________________________

Type of Clearance Required: □ Q □ L □ No Clearance

Type of Badge Received:

☐ LANL Generic Uncleared US Visitor
☐ LANL Generic Uncleared US Visitor Escort Required
☐ LANL Uncleared Site-specific
☐ LANL Uncleared / Cleared Foreign National
☐ Uncleared DOE
☐ DOE L
☐ DOE Q

SECTION I

In the performance of the referenced Subcontract and in order to comply with security requirements for subcontract workers outlined in DOE O 470.4B Chg 1, Safeguards and Security Program, LANS, LLC and the Subcontract worker agree to the following Individual Security Plan:

1. Subcontract worker shall comply with all security requirements outlined in this Individual Security Plan as well as any other security requirements discussed and briefed by their LANL host.

2. All non-U.S. citizen foreign national subcontract workers are required to have approval to work on-site from the LANL Foreign Visits and Assignments office PRIOR to their arrival at the Laboratory. They are required to present a valid passport and visa documentation before a badge will be fabricated and issued.

3. All required training shall be completed and documented prior to any work beginning. A record of all required and completed training follows.

<table>
<thead>
<tr>
<th>Course Required?</th>
<th>Course Title</th>
<th>Date Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Security</td>
<td>General Employee Training (GET) - On site 10 or more days</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LANL Emergency Procedures and Protective Actions - All</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Annual Security Refresher (ASR) – L &amp; Q-cleared Workers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comprehensive Security Briefing - L &amp; Q-cleared Workers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Export Control Fundamentals – Based on SOW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Substance Abuse Awareness – All</td>
<td></td>
</tr>
<tr>
<td>Course Required?</td>
<td>Course Title</td>
<td>Date Completed</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Workplace Violence Awareness</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Cyber Information Security</td>
<td>Initial Information Security Briefing</td>
<td>All Computer Users</td>
</tr>
<tr>
<td></td>
<td>Annual Information Security Refresher</td>
<td>All Computer Users</td>
</tr>
<tr>
<td>Protecting Classified &amp; Sensitive Information</td>
<td>Protecting UCNI - Users of Unclassified Controlled Nuclear Information (UCNI)</td>
<td>If access to UCNI will be required</td>
</tr>
<tr>
<td>Physical Security</td>
<td>The Outsider – Vault or Vault Type Room User (AIS Escorts)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vault or Vault Type Room User – Vault or Vault Type Room Users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LANL Site-Specific Training (list as appropriate)</td>
<td></td>
</tr>
</tbody>
</table>

4. A subcontract worker who will obtain a standard badge (non-Visitor or Generic) such as a DOE Q, DOE L, DOE Uncleared, LANL Uncleared Site-specific, or Cleared/Uncleared Foreign National badge shall successfully pass a drug test no more than 60 days before requesting and obtaining a standard badge.

5. Should the parties to the above referenced change, all applicable Foreign Ownership, Control or Influence (FOCI) security requirements associated with a Q clearance will be immediately applicable as required by DOE/NNSA. [Contact Melissa Abeyta regarding FOCI requirements at 505-665-1624]

6. Any badge provided by LANL under the above subcontract is strictly for use in the performance of the work outlined in this subcontract and the badge shall not be utilized for any other work or activities.

7. Subcontract worker shall notify LANL Personnel Security immediately if access to LANL is no longer required due to termination of subcontract, badge expiration, end of assignment or completion of a visit. Failure to return a badge will result in denial of future badging services to the badge holder.

8. When the subcontract is terminated, any associated security clearance will also be terminated.
By signature below, the responsible LANL line manager (RLM) and Subcontract worker acknowledge that all the security requirements contained herein have been briefed, read and agreed upon. A copy of this ISP shall be provided to the Subcontract worker.

Approved by LANL Manager (RLM)

___________________________  __________________  __________________
Printed Name                        Signature                        Date

Accepted by Subcontract Worker

___________________________  __________________  __________________
Printed Name                        Signature                        Date

SECTION II

Additional security requirements that shall be complied with while working for Los Alamos National Laboratory are outlined in the following pages.

Subcontract worker’s signature on this Individual Security Plan acknowledges consent to comply with these requirements; in addition to any facility-specific security requirements the LANL host may provide.
General Security
<table>
<thead>
<tr>
<th>Situation to Report</th>
<th>Whom to Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abandoned packages; low-flying aircraft</td>
<td>Protective Force</td>
</tr>
<tr>
<td>Emergency Operations</td>
<td>(667-437)</td>
</tr>
<tr>
<td>Unattended vehicles parked or operated in a suspicious manner or near laboratory facilities</td>
<td>Protective Force</td>
</tr>
<tr>
<td>Protective Force</td>
<td>(667-437)</td>
</tr>
<tr>
<td>Exhibits of security measures; presence and unattended protective equipment, or asking questions about the operations, carrying suspicion or threat conditions of those observing, suspicious or unknown persons, particularly those</td>
<td>Protective Force</td>
</tr>
<tr>
<td>Security Inquiry Team</td>
<td>(663-3509)</td>
</tr>
</tbody>
</table>

In addition to looking parked vehicles, workers should also get in the habit of inspecting their surroundings:

- Signs of tampering or indications of forced entry into doorways of windows.
- Unattended packages.
- Suspicious activities.

Laboratory workers should always be vigilant of their surroundings.
Professional from the STIP.

Incidents are bound to occur when humans work with processes. A quick response with appropriate reporting.

Why?

Security Incident Team (SIT) and to your supervisor.

All potential and actual incidents of security concern must be reported IMMEDIATELY to the Security Incident Team (SIT) and to your supervisor.
HOW TO HANDLE A VIOLENT SITUATION

If you believe the situation is life threatening or could result in bodily harm,
call 911 immediately.

Report the incident to Human Resources-Employee Relations.
The supervisor must also
be present and must assure the worker involved that they are safe.

A supervisor must act when a worker demonstrates violent behavior by having
behavioral patterns that are threats to workplace violence.

Workers should immediately as soon as possible by another employee or otherwise report

Reporting Concerning Behavior

- Concerned with a specific individual or group?
- Significant changes in social interactions (e.g., sudden withdrawal or seeming
  sadder)
- Changes in eating or sleeping patterns
- Excessive smoking or other drug use
- Involving family or friends
- Changes in work performance
- Notice of problems
- Sensing of potential or immediate danger
- Fierce outbursts or being easily provoked
- Reporting

Violence

- Physical or verbal
- Know the people with whom you work and notice when their behavior seems out of place

Preventing Workplace Violence

- Workplace violence consists of hostile or aggressive physical contact with another person.
- A determination of body gestures that present a threat to another person or potential threat would
Responding to an Active Shooter

The workplace should never be a dangerous place. Unfortunately, shootings occasionally happen.
Workers: Course #42995, Substance Abuse Policy and Procedure P732, for all Laboratory Training.

- Personnel Security 667-4264
- Human Resources/Employee Relations 917-667-8730

The manager must conduct the Personnel Security in accordance with the manager Personnel Security will determine if testing is appropriate, based on all circumstances. If the worker's manager is unavailable, the worker must notify the next level manager or Personnel Security. Notice:

When an individual returns to the Laboratory, he or she must complete a Substance Abuse Test within the bounds of their Laboratory Technical area.

The worker is driving any government-owned vehicle, including motorized equipment such as a forklift, on or off of Laboratory Property.

The worker is driving any government-owned vehicle, including motorized equipment such as a forklift, on or off of Laboratory Property.

For many years, the Laboratory has conducted substance abuse testing following accidents. Testing protocols lose Alarms.

Reporting Requirements for Vehicle Accidents
Security Help Desk: security@lanl.gov, 665-2002
Badge Office: badge@lanl.gov, 665-6901

Resources:

The Elk Grove workers may wear their security badges at the air.

A. Because Hot Rocks is housed in the Research Park, which is a leased facility adjacent to an bus stops and buses.

A. Park and Ride is public transportation. Laboratory workers should not wear their badges at the Hot Rocks Cafe?

A. Can I wear my badge on the Park and Ride bus?

If their badges are lost or stolen:
- Submit a Notification of Permanent Inactivation of Badge
- Notify a Notification of Permanent Inactivation of Badge
- Notify laboratory staff
- Notify any reason. Note: Workers on
- Not use their badges for deception or unauthorized
- Remove their badges and protect them from public view or

Every laboratory worker and visitor is issued a badge. Whenever cleared or uncleared, badge holders must follow Department of Energy and Laboratory rules regarding protecting their badges.

Badge Holder Responsibilities:
Reported (via secure means) to the Security Inquiry Team (SIT).

If a potential incident of security concern and must be immediately
Foreign national worker has entered a non-secure or secure LANL building that was not
Entry into an unauthorized building by a foreign national may be a security event. It a

Reporting Requirements

With the exception of OCS/PA.
Specific Access Agendas, Maps, Escort Forms, and coordination
process as required approval of the following: DIVA. Form 1276.
Generally provided: Contact OCS/PA for guidance with the
Access to secure areas by unapproved foreign nationals is
Secure Areas

Update the approved DIVA Record.
If a foreign national needs access to a building not listed on DIVA, he or her host can
Foreign national access a LANL Facility
Access to the database for International Visitors and Assignments (DIVA) must be approved before
the assignment office (OCS/PA) will meet with a LANL representative. The
Assignment Office (OCS/PA) must be met with by the Office of Counterintelligence/Foreign Visits
Foreign national visitors and visitors (including those who have U.S. permanent

Foreign National Access into LANL Buildings
Security Help Desk: security@lanl.gov 665-2002
Foreign Visits and Assignments: 665-1772
Resources

Non-US visitors are controlled to access facilities that are specifically listed in their DVA.

Authorization the Badge Office to issue badges to foreign national visitors.

Prior to work or visits, following DVA approval, foreign visitors and assignees (FVA) are processed through the badge office for a standard site visit. Approval and badges prior to their arrival and must be approved before exiting the site.

All non-US visitors and assignees must be approved by the Badge Office.

Laboratory facilities, whether owned or leased, may not issue badges. Any exceptions must be authorized by the lab management.

Museum, which is an open area where the general public is not expected to be, with the exception of the Energy Science Area, (ESPA), Central Lake, Central Park Square, and the White Rock Foundation.

Commercial, commercial parks, and the White Rock Foundation.

Lab employees may own掌控, control, and have access to leased facilities.
Police Department

Violation of these rules may result in immediate arrest.

Access to Area:

- Employees, volunteers, and visitors are required to use designated entrances and exit only at designated times.
- Access to areas is controlled and monitored by security personnel.
- Employees, volunteers, and visitors are required to present photo identification at all times.
- No admittance to areas without proper identification.

Areas:

- Restricted Areas - Employees, volunteers, and visitors are not allowed to enter these areas.
- Controlled Access Areas - Employees, volunteers, and visitors are required to obtain a pass for access to these areas.
- Public Areas - Employees, volunteers, and visitors are allowed to enter these areas.

Illegal Items:

- Prohibited items include: firearms, knives, and other sharp objects, and regulated substances.
- Possession of illegal substances is strictly prohibited.

Prohibited Articles:

- Prohibited articles include: firearms, knives, and other sharp objects, and regulated substances.
- Possession of illegal substances is strictly prohibited.

Open vs. Controlled Access Areas:

- Employees, volunteers, and visitors are required to use designated entrances and exit only at designated times.
- Access to areas is controlled and monitored by security personnel.
- Employees, volunteers, and visitors are required to present photo identification at all times.
- No admittance to areas without proper identification.

Areas:

- Restricted Areas - Employees, volunteers, and visitors are not allowed to enter these areas.
- Controlled Access Areas - Employees, volunteers, and visitors are required to obtain a pass for access to these areas.
- Public Areas - Employees, volunteers, and visitors are allowed to enter these areas.

Illegal Items:

- Prohibited items include: firearms, knives, and other sharp objects, and regulated substances.
- Possession of illegal substances is strictly prohibited.

Prohibited Articles:

- Prohibited articles include: firearms, knives, and other sharp objects, and regulated substances.
- Possession of illegal substances is strictly prohibited.
Security Inquiry Team and the worker's line management.

Inspections. Failure to do so may result in a security incident and notification of the worker. The worker must cooperate with and follow the instructions of the Protective Force during the inspection and the surrounding area as necessary.

Vehicle and the surrounding area as necessary.

Upon completion of the inspection, the team will either:
- Secure to the roof of the vehicle.
- Inspect the engine compartment (under the hood and chassis).
- Inspect the engine area, which includes a canine team, will.
- Control devices.
- A force officer will notify a driver to pull over to a search.

Random Vehicle Inspections
Resources

- Security Inquiry Team at 667-3000.
- The Protective Force at 667-4437.
- To report unauthorized photography, contact Mater Protection Group at 667-5108.
- For more information, contact the Classified Resources.

Photography on Laboratory Property

Workers who see photography on laboratory property should:

1. Request prior approval by electronically submitting Form 1897PA.
2. Carry a copy of the approved Form 1897PA while taking photographs and include cell phones with cameras.
3. Present the approved Form 1897PA to anyone who requests to see it.

Photography immediately notify the Protective Force or Security Inquiry Team to report unauthorized photography.
The information and the requirements for protecting that information.

Recommended. It is the sender's responsibility to ensure that the recipient understands the sensitivity of

Encrypt must be used.

Over telecommunications circuits (including facsimile)

Restrictions apply to passwords, authentication, the access control, encryption, and offline storage.

UNCLl should be restricted to only those that have a need to know. Examples of

Electronic media

Non-electronic media

As a rule, keep the cabinet, or safe (to prevent unauthorized disclosure). The locked receipt

When using UNCLl, an authorized individual must maintain physical control over the material to

Restricted to have utilized such items, and security relating to such items.

The atomic energy act, such information may concern nuclear material, weapons, components,

Government information whose unauthorized dissemination is prohibited under section 186 of

Unclassified Controlled Nuclear Information (UCNI) is certain undiscussed but sensitive
Resources

- Commodities and software exports
- Export of commodities and software from the Laboratory, and maintaining control records of
- Classification, designating license exceptions, preparing shipping documents, applying all
- The Laboratory’s Customs Office is available to help with obtaining licenses, commodity

Customs Office

- Year’s (2) civil penalties; or (c) administrative sanctions, such as seizure of the items in question.
- Licenses include (1) annual sanctions of fines up to $10 million and imprisonment for up to 10
- Both the Laboratory and workers may be liable for control requirements are violated.
- (e) The Department of Commerce, Department of Justice, and Nuclear Regulatory Commission.

Violations of Export Control

- country,
- technology to a foreign national in the US is deemed to be an export to that person’s home.
- One can “export” something to a foreign national without leaving the country. Transfer of

Deemed Export

- materials to reduce the serious international impact of foreign demand.
- goods where necessary to protect the domestic economy from the excessive drain of scarce
- international obligations, and
- goods and technology to further the foreign policy of the United States or fulfill its dedicated
- another country of combination of countries.

Export Control

- Export Control is intended to restrict the export of
IMPORTANT

Rev 2 (05-22-2015)

Page 26 of 31

Portale Electronic Devices

Resources

- Two-way radios and radios
- Some medical devices (e.g., heart monitors)
- Laptop or portable computer
- Digital audio players (e.g., iPods)
- Copiers or scanners with hard drives
- Cell phones and personal digital assistants

(Conditional Approrpried

Cameras (e.g., all types of external and internal devices such as webcams, webcams, etc.)
- Control of external drives (e.g., anti-malware drives)
- Samples of controlled articles

Controlled Articles are standalone devices that can read and/or transmit data. Some examples include:

- USB memory devices (thumb drives, memory sticks, jump drives)
- Flash memory (e.g., PC cards, SD memory cards)
- External hard drives
- CD/DVD white drives
- Device, PEDS included:

Electronic Storage Devices (PEDs) and Controlled Articles

Electronic Storage Devices (PEDs) can potentially transmit or transport sensitive unclassified

Information (Cyber) Security Help Desk: 665-2002, Cybersecurity@NRL.gov

Information (Cyber) Security Help Desk: 665-7955, Cybersecurity@NRL.gov
Send questions regarding network security to csl@lan.gov

665-3355. After hours or on weekends, page the On-Call Duty Officer at 505-499-0156.

Report all potential information security incidents to the Security Inquiry Team (SIT) at 505-

Reporting an Information Security Incident

- must never be shared;
- cannot be names of common words (those found in a dictionary), and symbols;
- must contain a variety of characters (upper-case letters, lower-case letters, numbers, and
- must be a minimum of 8 characters and be changed at least every 180 days;

Your Computer: Reusable Passwords:

- Cannot contain a password previously used. Changing strong passwords is important in preventing unauthorized access to your computer. When a token password is used, a token can be used instead of the password to ensure one-time password security.

Steps to Take

1. Download and install the most recent operating system security patches.
2. Do not open unknown email attachments or click on suspicious links.
3. The laboratory’s Yellow Network prevents most cyber attacks. Computer users are en
Computer User Responsibilities

1. **Follow the established guidelines for destroying data and safeguarding computer equipment.**

2. **Configure your system to automatically log off after 15 minutes of inactivity.**

3. **Enable screen saver protection whenever you leave your computer.**

4. **Contact your IT department manager and promptly report any security or system issues.**

5. **Understand the need-to-know concept before you share information with others.**

6. **Know the sensitivity level of the data you process and how to complete required initial and annual information security training.**


8. **Get to know your Laboratory’s Information Security Program.**

9. **Heed the following guidelines will help protect the Laboratory’s information security.**

10. **Coordinating these activities with your OCSR and property administrator.**
Remember: Compilations of one or more unclassified attachments and a string of unclassified emails may make the entity of an email classified.

Pills: Pill emails containing Pill must be encrypted before sending outside the laboratory.

Network, no encryption is required but it is recommended.

IST: Validated encryption software (Enutad). When transmitted with LANs yellow
LNCI: When transmitted electronically outside LANs, LNCI must be encrypted with

ODO: Indicate ODO on the first line before the body of the letter.

Personally Identifiable Information (PII), have additional requirements:

- Do not distribute controlled unclassified information (CUI).
- Keep in mind that emails with controlled unclassified information (CUI) may be unauthorized to receive.

Review Before Sending

Unclassified mail classified:

Workers must ensure that email containing classified information is not transmitted over

Protecting Emails and Attachments
Social Networking, Privacy and Computer Security

http://lansky.gov/security/privacy/ptr/Internet/SSL/SSL_Examples
Organizational Computer Security Representatives,
Computer Security Help Desk, cybersecurity@lansky.gov

Reasons
Avoid accessing social networking sites from your work computer for non-business-related
Be careful of pop-up windows and links. Verify their legitimacy before clicking on them.
Delete cookies every time you leave a social networking site.
Run updated virus protection software regularly.

Some Tips for Computer Security

Do not share details about your laboratory work.

Some Tips for Privacy

Phishing is the attempt by hostile individuals
You have the control over your personal information once you post it online. Keep the
Lab workers should be especially careful of

Consider your “friends” before allowing a “friend request” into your network. You

Twitter

Facebook

LinkedIn

Rev 2 (05-22-2015)