Sandia-Controlled Premises Access and Escort procedures

Access to SNL/NM is controlled through the use of authorized badges. The most common are the Local Site Specific Only (LSSO) badges and the HSPD-12 Credential. Badges are issued based on the areas the person will need to access and the type of clearance held.

- If you are being escorted - remain with your escort at all times when in a Limited or more restricted area.
- Uncleared individuals may only be escorted by appropriately cleared and badged U.S. citizens who are familiar with Sandia safety and security-related corporate procedures that apply to the areas being accessed.
- Uncleared foreign nationals may only be escorted by appropriately badged Sandia employees who are U.S. citizens identified as escorts on the Foreign National Request Security Plan (FNRSP) and may only access areas listed on the approved FNRSP.

Badge Procedures/Best Practices

- Your badge is government property; return it when your employment is terminated, security clearance status changes, or it is no longer needed.
- Badge should be worn at all times, above the waist, photo side out, and in front of your body; otherwise remove the badge or prevent visual access.
- Do not use your badge as means of identification for unofficial purposes.
- Protect your badge against loss, theft, misuse or alteration and report lost or stolen badges to Security Connection @ 321 from a Sandia phone, or 505-845-1321.

Government or Sandia Property Protection

- Misuse of Sandia or Government-owned equipment (computers and vehicles) is considered “waste, fraud, and abuse” and may be a punishable offense.
- Individuals are subject to search. This includes unannounced package and vehicle inspections.
- Do not park in unauthorized areas (e.g., Reserved, Handicap, Security).
- Follow all posted speed limits (if not posted, the speed limit is 15 mph).
- Smoking is not allowed on Sandia-controlled premises.

Controlled and Prohibited Articles

CONTROLLED ARTICLES: Articles that are controlled because of their potential to be used to record, store, or transmit information without authorization. Examples include recording equipment, electronic equipment with a data exchange port capable of being connected to automated information system equipment or radio-frequency-transmitting equipment (including Bluetooth and cellular devices). Government-owned computers procured through SNL's JIT purchasing system are exempt from controlled-article registration requirements. For additional guidance, refer to ISS100.5.1, Manage Controlled and Prohibited Articles.

PROHIBITED ARTICLES: Alcohol or other intoxicants; illegal drugs and paraphernalia; weapons, explosives, incendiary devices, and other dangerous instruments or materials likely to produce injury or damage to persons or property are not allowed anywhere on Sandia controlled premises. For additional guidance, refer to ISS100.5.1, Manage Controlled and Prohibited Articles.

Prompt Reporting to Security Connection

- If you See Something, Say Something! Promptly notify your escort or manager of security concerns (attempts to gain unauthorized access to the facility or to classified information or matter).
- Report lost or unprotected classified or sensitive unclassified information immediately.
- Security Connection is available 24/7/365.

In Case of an Emergency

- Report emergencies to 911 from a Sandia phone or 505-844-0911.
- Report non-emergencies to 311 from a Sandia phone or 505-844-0311 or 845-0311.

Protection of Unclassified Controlled Information (UCI)

- Unclassified Controlled Information (UCI), which includes Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI) access is given to a person who...
needs it to perform his/her duties (need to know) and must be properly marked, stored, and protected. Access to UCI does not require a clearance. See CP IM100.2.5 Identify and Protect Unclassified Information.

- Personally Identifiable Information (PII) should always be protected and limited to official business. See CP IM100.2.6 Control Personally Identifiable Information.

**Working With Classified**

Access to classified matter is restricted to persons with an access authorization (security clearance) and a “need to know”. All classified documents must be clearly identified on the outside and require special handling and protection. You can identify classified documents by the cover sheets shown here. All documents should be marked clearly on the top and bottom of each page. See Corporate Policy (CP) ISS100.1.1 Identify Classified Information.

When working with classified information, use only computers on the Sandia Classified Network (SCN) or an approved stand-alone system. Home computers are not considered approved, stand-alone systems, even for use with Sandia’s unclassified information.

Information processed on a classified computing system is considered classified at the system level and category (also known as “system high”) until it’s reviewed by an authorized Derivative Classifier (DC). Such information should be marked and controlled appropriately until it has been reviewed for classification.

When exporting any data from a classified system to an unclassified system (whether electronically or by use of electronic media), an Authorized Transfer Point (ATP) must be used and approved processes must be followed.

Use secure forms of telecommunication (classified fax machine, copier and other electronic transmissions).

Get a formal review if you intend to release information to an uncontrolled, widespread, unknown, or public audience. This includes information intended for release to Congress. You must obtain a formal Review and Approval (R&A).

**Sandia National Laboratories/New Mexico and Remote Sites**

**Initial Security Briefing (SEC050)**

As an individual with access to Sandia-controlled premises and other U.S. Department of Energy (DOE) facilities, you are critical to ensuring a safe and secure workplace. This briefing provides an overview of your security responsibilities.

**Mission and Program Areas of Sandia National Laboratories**

Sandia National Laboratories unique mission responsibilities in the nuclear weapons (NW) program create a foundation from which we leverage capabilities, enabling us to solve complex national security problems.

As a multidisciplinary national laboratory and federally funded research and development center (FFRDC), Sandia accomplishes tasks that are integral to the mission and operation of our sponsoring agencies by:

- Innovating and discovering new technologies to strengthen the nation’s technological superiority
- Creating value through products and services that solve important national security challenges
- Informing the national debate where technology policy is critical to preserving security and freedom throughout our world

Major program areas include defense, nonproliferation, climate, infrastructure, homeland security, counter-terrorism, cybersecurity, and nuclear weapons.

**Safeguards and Security Program Responsibilities**

The Safeguards and Security Program is responsible for access control, physical protections, information protection, protective force, education and awareness, security incident management, classification, classified matter protection and control, operations security, and international travel and risk management.