Initial Security Briefing

This Initial Security Briefing provides a concise overview of security responsibilities, and is intended for all individuals accessing Sandia National Laboratories at all sites.

Safeguards + Security

Mission and Program Areas of Sandia National Laboratories

Our unique 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 multimission 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:

- Anticipating and resolving emerging national security challenges
- 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 security operations.

WHO	General Access Area (GAA)		Property Protection Area (PPA)	Limited Area (LA)	Vault-Type Room (VTR)
	Public	Non-Public			
DOE Badged, Cleared individual	✓		✓	✓	Access list or escort **required**
DOE badged, un-cleared individual	✓		✓	Escort **required**	Escort **required**
Unbadged individual (incl. children)	✓	Only as approved for **certain events**			**NO**
Uncleared foreign national	FNR SP may be required	Approved FNR SP and escort **required** prior to access		Approved FNR SP **and** escort **required** prior to access	**NO**

Controlled Articles

A **controlled article** is an item that is capable of recording information or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment). Controlled articles must have **prior authorization** before they may be brought into a limited or more restrictive area.

Sandia-issued controlled articles not already authorized in Sandia policy must be registered/approved through the **Controlled Articles Registration Process (CARP)** prior to use within limited or more restrictive areas.

Personally owned controlled articles not already authorized in policy are **not allowed** in a limited or more restrictive area.

Prohibited Articles

A **prohibited article** is an item administratively restricted from being introduced onto Sandia-controlled premises. Prohibited articles include, but are not limited to: **firearms, explosives, pepper spray, stun guns, dangerous weapons, instruments likely to produce substantial injury to persons or property, hazardous materials, alcohol,** or any other item **prohibited by law.**

Prohibited articles are not allowed on any Sandia-controlled premises, **including parking lots.**

WHAT	GAA	PPA	LA	VTR
Sandia-issued controlled articles	✓	✓	Authorization **required** prior to introduction	Authorization **required** prior to introduction
Personally owned controlled articles	✓	✓	**NO**	**NO**
Prohibited articles	**NO**	**NO**	**NO**	**NO**

Mobile Devices

A mobile device is any portable computing device that has a small, easily carried form factor; possesses onboard sensors that allow the device to capture audio or video information; does not utilize a desktop operating system safeguarded by a NNSA Cyber Security Program; is designed to operate wirelessly; possesses local, non-removable data storage; and that is powered-on for extended periods of time with a self-contained power source. **Examples include cell phones, tablets, some smart watches, and more.**

Members of the Workforce may bring mobile devices into a limited area as long as **Bluetooth and WiFi are disabled**. Mobile devices are prohibited from entering any location marked **Secure Space** at any time, and may only be stored in marked, approved storage locations.

Only **Sandia-managed mobile devices** are allowed anywhere in a limited area not marked Secure Space or a more restrictive area. **Personally owned mobile devices** are only allowed in limited area ***common areas,*** including hallways, breakrooms, storage locations, and outside.

Visitors to Sandia are not permitted to bring mobile devices into limited areas.

Medical Portable Electronic Devices

Medical Portable Electronic Devices (MedPEDs) are not permitted within a limited or more restrictive area until approved following an evaluation for **technical security vulnerabilities**.

Approved devices may be brought into limited areas only in accordance with mitigations or guidance as provided (e.g., 'Airplane Mode') following the evaluation. **Until a MedPED is approved, it is not authorized to enter a limited area.**

For more information on obtaining a technical review, contact the MedPEDs team at medpeds@sandia.gov or visit medpeds.sandia.gov.

WHAT	GAA	PPA	LA	VTR
Sandia-managed mobile devices	✓	✓	✓	*SECURE SPACE* **NO**
Personally owned mobile devices	✓	✓	**Common Areas Only**	**NO**
Medical Portable Electronic Devices	✓	✓	Authorization **required** before introduction. **Contact medpeds@sandia.gov**	

Sandia National Laboratories

U.S. DEPARTMENT of ENERGY
NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2024-XXXXXM

security.sandia.gov

Protection of Information

While at Sandia and thereafter, it is your responsibility to mark and protect sensitive information from unauthorized release, including but not limited to:

- **Controlled Unclassified Information (CUI)**, a type of sensitive federal government information subject to dissemination and safeguarding controls based on a **law, regulation or government-wide policy (LRGWP)**. CUI must be protected and is releasable only to those with a lawful governmental purpose (LGP) who are authorized for access in accordance with the LRGWP. You may also encounter ***Official Use Only (OUO)*** information, a legacy marking of sensitive federal government information that is no longer in use at Sandia. OUO is protected as CUI. For further guidance, visit *cui.sandia.gov.*

- **Critical information**, which includes specific facts about intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment, and is determined by Sandia's OPSEC program. Approved critical information is protected as CUI. For further guidance, contact *opsec@sandia.gov.*

- **Classified information or matter**, access to which is restricted to persons with both a valid **access authorization** (aka security clearance) and **"need to know"**. Classified information is subject to specific requirements for identification, use, protection, dissemination and disposal. Classified markings must be clearly affixed to each piece of material or page indicating category and level of sensitivity. When transmitting, use secure forms of telecommunication. When working with classified information, only use computers on approved classified networks or an approved stand-alone system. For classified computing guidance, contact your **Cyber Security Representative or 3CSi**. Follow appropriate marking and protection requirements until reviewed by an authorized **Derivative Classifier (DC)**.

Releasing Information Outside SNL

Get a formal review. If you intend to release information to an uncontrolled, widespread, unknown, or public audience, the information must go through the formal **Information Release (IR)** process. This includes information intended for release to Congress. For further guidance, contact Security Connection.

Sandia-Controlled Site Control Access

Access to Sandia National Laboratories (SNL) is controlled by DOE authorized badges. The most common are cleared **DOE PIV (aka HSPD-12)** credentials and cleared/uncleared **Local Site Specific Only (LSSO)** badges. Badges identify the holder's clearance status, which in turn identifies the types of information and areas the individual may access.

Sandia Members of the Workforce and visitors **must not vouch** others into pedestrian access control points (turnstiles, gates, doors, etc.). Everyone MUST swipe or present his/her badge at each access control point when entering buildings, rooms and other security areas.

Before an uncleared foreign national may access DOE sites, information, cyber networks, or technologies (physically or remotely), a **Foreign National Request Security Plan (FNR SP)** that identifies access needs, specific locations being accessed and identification of hosts, cohosts, and/or approved escorts must be submitted and approved. For more information, contact the **Foreign Interactions Office** at *fionm@sandia.gov.*

Category	Level		
	Top Secret (TS)	Secret (S)	Confidential (C)
Restricted Data (RD)	Q only	Q only	Q and L
Formerly Restricted Data (RD)	Q only	Q and L	Q and L
Transclassified Foreign Nuclear Information (TFNI)	Q only	Q and L	Q and L
National Security Information (NSI)	Q only	Q and L	Q and L
Degree of Damage	**Exceptionally Grave**	**Serious**	**Damage**

Security Area Escorting Procedures

- The persons under **escort** must always remain with their escort in limited or more restrictive areas. **Escorts must be appropriately cleared and badged U.S. citizens** who are familiar with Sandia safety and security-related laboratory procedures that apply to the areas being accessed.
- While escorting, escorts and uncleared individuals must display the red and black **"U" and "E"** cards along with their authorized badges.
- **Uncleared foreign nationals** can be readily identified by bright red LSSO badges. These individuals may only be escorted by individuals **authorized** on the **FNR SP**.

Badge Procedures & Best Practices

- Your badge is **government property**; return it when your employment is terminated, clearance status changes, or it is no longer needed.
- Badge must be worn conspicuously, photo side out, above the waist and front of your body.
- Remove or obscure badge from visual access when not on SNL/DOE premises.
- **Do not use your badge as means of identification** for unofficial purposes.
- Protect your badge against **loss, theft, misuse or alteration**.
- Report **lost or stolen badges immediately** to Security Connection.

Security Notice

- Misuse or theft of SNL or Government equipment could be considered **"waste, fraud, and abuse"** and may be a punishable offense.
- All individuals are **subject to search** of their persons, hand-carried items, and vehicles upon entering or leaving Sandia controlled premises.
- 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**).
- Use of **tobacco products** is not allowed on Sandia-controlled premises.
- Comply with all gate entry protocols (e.g., staffed, automated, vehicle, military).
- Only government-plated, handicap, executive privilege, or contractor vehicles with a lawful purpose may enter Limited Areas.

Emergencies, alarms, life-threating situations, ...call 911

From any SNL/NM landline..... **505.844.0911**
In SNL/CA **925.294.2222**
Non-emergencies: **311**
From any phone **505.844.0311**

Reporting Concerns, Incidents, and Questions, contact Security Connection:

From any Sandia landline phone **321**
From any phone **505.845.1321**