<table>
<thead>
<tr>
<th>WHO</th>
<th>General Access Area</th>
<th>Security Area</th>
<th>Vault Type Room (VTR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public Badge not required</td>
<td>Non-Public Badge required</td>
<td>Property Protection Area (PPA) Badge required</td>
</tr>
<tr>
<td>Q-cleared individual (with SNL LSSO badge or DOE HSPD-12)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>L-cleared individual (with SNL LSSO badge or DOE HSPD-12)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Uncleared individual (with SNL LSSO badge)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Children / Friends</td>
<td>✓</td>
<td>Only as approved for certain events</td>
<td></td>
</tr>
<tr>
<td>Uncleared foreign national</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### WHO
- **Q-cleared individual**: with SNL LSSO badge or DOE HSPD-12
- **L-cleared individual**: with SNL LSSO badge or DOE HSPD-12
- **Uncleared individual**: with SNL LSSO badge
- **Children / Friends**: Only as approved for certain events
- **Uncleared foreign national**: A Foreign National Request Security Plan (FNRSP) may be required before working with an uncleared foreign national. FNRSPs list areas they may access. For additional guidance contact the Foreign Interactions Office (505-844-8263).

### WHAT

<table>
<thead>
<tr>
<th>WHAT</th>
<th>Public</th>
<th>Non-Public</th>
<th>Property Protection Area (PPA)</th>
<th>Limited Area (LA)</th>
<th>Vault Type Room (VTR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM/FM radio</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Electronic medical device capable of transmitting or storing data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sandia-owned PEDs (blackberry w/credential, iPad, and iPhone)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sandia-owned camera</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Non Sandia-owned Portable Electronic Devices (includes personal, business, &amp; other government)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personal weapons/Alcohol</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
</tr>
<tr>
<td>Marijuana (medical, extracts such as CBD, etc.)</td>
<td>Prohibited Article</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Someone else’s prescription medication</td>
<td>Prohibited Article</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Before bringing a laptops or other electronic devices into a VTR, ask the VTR owner for more information.

**Some areas of a GAA or PPA may not be approved for PEDs. Always be aware of local signage.

Comply with all posted local (such as facility-specific) restrictions and control measures for controlled devices and media.

### SEC050: Initial Security Briefing
**Sandia National Laboratories (All Sites)**
**Revised April 2020**

This is an overview of site specific security responsibilities for all individuals given access to Sandia National Laboratory (SNL) controlled premises.

### 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.

### Controlled and Prohibited Articles

**Controlled Articles** are items that are controlled because of their potential to be used to record 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 the Controlled Article Registration Process (CARP).

**Prohibited Articles** are items that are not allowed anywhere on Sandia controlled premises that are likely to produce injury or damage to persons or property. Examples include dangerous instruments or materials, alcohol or other intoxicants; illegal drugs and paraphernalia; weapons, explosives, or incendiary devices.

For additional guidance or to report unauthorized articles, contact Security Connection.
Security Notice
- Comply with all gate entry protocols (e.g., staffed, automated, vehicle, military).
- **Vouching is only allowed at vehicle gates**, not at pedestrian access-control points (gates, turnstiles, doors etc.) or facilities with automated access controls.
- Misuse or theft of SNL or Government equipment (e.g., computers, vehicles) 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.

Sandia-Controlled Premises Access and Escort procedures
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.
- Persons under escort must always remain with their escort in Limited or more restricted 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 unclesred individuals must display the “U” and “E” cards along with their authorized badges.
- **Uncleared** foreign nationals require a Foreign National Request Security Plan (FNRS) which identifies who is authorized to escort the foreign national and the areas approved for access.

**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 to Security Connection.

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.

Protection of Unclassified Controlled Information (UCI)
- Access to Unclassified Controlled Information (UCI), which includes Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI) may be 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. For further guidance contact Security Connection.
- Personally Identifiable Information (PII) should always be protected and limited to official business. For further guidance contact Security Connection.

Working With Classified

<table>
<thead>
<tr>
<th>Category</th>
<th>Top Secret (TS)</th>
<th>Secret (S)</th>
<th>Confidential (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted Data (RD)</td>
<td>Q only</td>
<td>Q only</td>
<td>Q and L</td>
</tr>
<tr>
<td>Formerly Restricted Data (FRD)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
<tr>
<td>Transclassified Foreign Nuclear Information (TFN)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
<tr>
<td>National Security Information (NSI)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
</tbody>
</table>

| Degree of Damage                     | Exceptionally Grave | Serious | Damage |

Access to **classified matter** is restricted to persons with an access authorization (security clearance) and a “need to know”. All classified matter must be clearly identified and require special handling and protection. Classified markings must be affixed to the matter to identify sensitivity and who is permitted to access it. All sensitive documents should be marked clearly on each page. For further guidance contact Security Connection.

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

When working with classified information, only use computers on **approved classified networks** (e.g., Sandia Classified Network [SCN]) or an approved stand-alone system. For guidance on classified computing, contact your Cyber Security Representative or 3CSi (505-284-3274). Follow appropriate marking and protections requirements at all times, even on classified systems. (e.g., mark ‘system high’ until reviewed by an authorized Derivative Classifier [DC], then update the marking as necessary).

**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 Review and Approval (R&A) process. This includes information intended for release to Congress.

**Security Concerns** (attempts to gain unauthorized access to areas or information, lost or unprotected classified or sensitive unclassified information, etc.) should be reported immediately to Security Connection. Available 24/7/365.

SNL/NM : Report emergencies to 911 from a Sandia phone or 505-844-0911
SNL/CA: Report emergencies to 911 from a Sandia phone or 925-294-2222
Report non-emergencies to 311 from a Sandia phone or 505-844-0311 or 505-845-0311.