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, smart watches, e-readers, 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 for MEDPEDs, contact Telecommunications Security at telecomm@sandia.gov.
Protection of Information

While at Sandia and thereafter, it is your responsibility to protect certain types of information from being disclosed to those without a need-to-know. The following types of information require protection:

- **Critical information** may include 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. For further guidance, contact opsec@sandia.gov.

- **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 and must be properly marked, stored, and protected.

- **Personally Identifiable Information (PII)** should always be protected and limited to official business.

- **Classified information or matter** access 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].

<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 (RD)</td>
<td>Q Only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
<tr>
<td>Transclassified Foreign Nuclear Information (TFNI)</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>

### 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.

### Sandia Controlled Escorting Procedures

- The 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 uncleared individuals must display the red and black “U” and “E” cards along with their authorized badges (pictured).

- **Uncleared** foreign nationals require a Foreign National Request Security Plan (FNRSP) which identifies who is authorized to escort the foreign national and the areas approved for access. These individuals can be readily identified by bright red LSSO badges. For further guidance, consult your manager or Deployed Security Professional.

### 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).

### Emergencies, alarms, life-threatening situations:

- Call 911 from any Sandia landline phone
- In SNL/NM, call 505-844-0911 | In SNL/CA, call 925-294-2222
- **Non-emergencies:**
  - Call 311 from a Sandia phone
  - 505-844-0311 or 505-845-0311 from any other phone

---

**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 Review and Approval (R&A) process. This includes information intended for release to Congress. For further guidance, contact Security Connection.