Advanced Change Directive (ACD) 470.6 – *Frequently Asked Questions*

Phase 2

PEDs.sandia.gov

TIMELINE

What is the timeline for Phase 2 implementation?

Sandia must complete Phase 2 full implementation by January 31, 2021. However, in order to establish a grace period for reported mobile device incidents, Sandia leadership is currently planning to activate Secure Space, including all the requirements of Phase 2, in late November of 2020. A decision will be made in early November if either the implementation or activation date will change due to the role of Sandia-owned mobile devices in COVID-19 contact tracing.

SECURE SPACE

What is Secure Space?

Following is the NNSA directive definition of Secure Space:

- NNSA Secure Spaces include all Material Access Areas, Protected Areas, Vault-Type Rooms, special designated areas, and areas requiring recurring TSCM services. NNSA Secure Spaces also include Limited Areas, or any portion thereof, to include an individual room, within which, any National Security System (i.e., classified processor) is physically present. Sufficient electromagnetic and acoustical isolation can be used to segregate Secure Spaces within larger Limited Areas.
- Areas (Buildings, Rooms, etc.) where classified discussions no matter the level take place.
- Classified Video Teleconference rooms and Classified Skype rooms.

In simple terms, Secure Space is any location that has classified discussions and/or processing. Project teams have characterized every building within limited areas to identify these spaces. Apart from a few exceptions where only a portion of a building has been identified as Secure Space, *most buildings inside a limited area will be designated entirely as Secure Space*. All Secure Spaces will be well marked with signs.

Can any mobile devices be brought into Secure Spaces, once they are activated?

No mobile devices, regardless of ownership (personally owned, Sandia owned or other government agency [OGA] owned), can be brought into Secure Space once it has been activated.

Is there such a thing as 'non-Secure Space'?

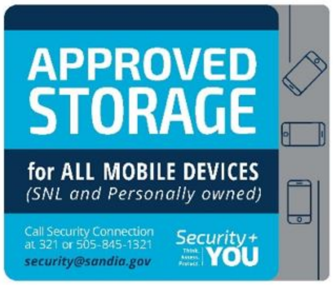
Not really. The directive only defines Secure Space. However, the directive *does* outline some very specific requirements for separation between Secure Space and the space it borders (which by process of elimination could be considered 'non-Secure Space').

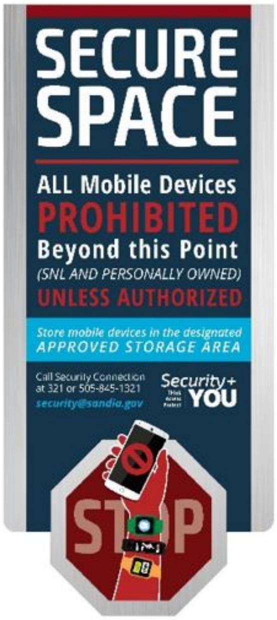
Can mobile devices be brought into limited areas?

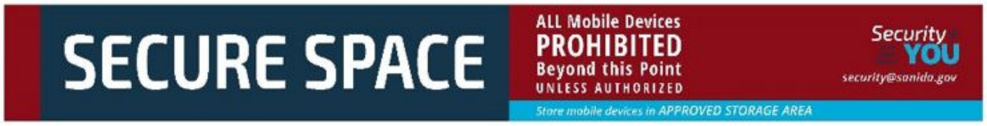
Yes. Once Phase 2 is implemented, both Sandia owned and personally owned mobile devices may be brought into a limited area boundary provided they don't enter areas designated as Secure space. Since laboratory policy states that classified conversations cannot occur outside, even if within the limited area, it will be permissible for a mobile device to be brought, for example, through a turnstile into Tech Area 1 in New Mexico, provided that all other requirements are satisfied (Bluetooth and WiFi disabled; individual is authorized).

Do Bluetooth and Wi-Fi still need to be disabled in limited areas outside of Secure Space?
Yes, as stated above, the policy regarding Bluetooth and Wi-Fi within limited areas remains in effect—Bluetooth and Wi-Fi must be disabled inside limited areas. (For Sandia owned devices, Wi-Fi may be enabled *only* in an approved Wireless Access Zone.)

How will I be able to distinguish Secure Space from non-Secure Space?
Clear and standard signage will be posted which 1) identifies the area as Secure Space and 2) states what devices are prohibited.


APPROVED STORAGE
for ALL MOBILE DEVICES
(SNL and Personally owned)
Call Security Connection at 321 or 505-845-1321
security@sandia.gov
Security + YOU


SECURE SPACE
ALL Mobile Devices
PROHIBITED
Beyond this Point
(SNL AND PERSONALLY OWNED)
UNLESS AUTHORIZED
Store mobile devices in the designated APPROVED STORAGE AREA
Call Security Connection at 321 or 505-845-1321
security@sandia.gov
Security + YOU
STOP

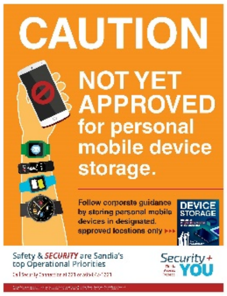


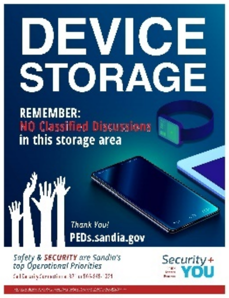
STORAGE

Is additional mobile device storage being installed for Phase 2?
The Project Team is currently installing more than 150 new storage units—both external and internal—around Secure Space entrances. Installation should be completed by the end of October. Visit PEDs.sandia.gov for more information on mobile device storage and signage.

I see new internal storage boxes being installed, but they are marked with signs saying they are not yet approved for use. Why can't we use them now?
Until Phase 2 is activated, the Phase 1 policies are still in place, meaning that only the temporary, designated storage locations are currently approved for use. The new internal storage boxes located inside limited area buildings will be approved for use as soon as Secure Space is activated.

How can I be sure which storage locations are OK to use right now, and which are not yet approved?
All new storage locations should be marked with one of these two signs. Existing, *internal* storage units that are not marked with a sign should be treated as 'not yet approved' for personally owned devices. Only *external* storage units and the designated, internal storage locations marked with the blue sign are approved for use for personally owned devices until Phase 2 is implemented.


CAUTION
NOT YET APPROVED
for personal mobile device storage.
Follow corporate guidance by storing personal mobile devices in designated, approved locations only ▸▸▸
DEVICE STORAGE
Safety & SECURITY are Sandia's top Operational Priorities
Security + YOU


DEVICE STORAGE
REMEMBER:
NO Classified Discussions in this storage area
Thank You!
PEDs.sandia.gov
Safety & SECURITY are Sandia's top Operational Priorities
Security + YOU

Why are locks being removed from some of the external storage boxes?
Locks were removed in order to ensure that the boxes are available on a first come, first served basis and to eliminate costs associated with key maintenance and replacement.

What is being done with old/current storage boxes?
Old/current storage boxes located in Secure Space are NOT approved for use since mobile devices are not permitted in Secure Space. Additionally, old/current storage boxes that do not meet building codes will be removed. The Project Team will work with the owners on options for reuse.

Can my organization order and install mobile device storage solutions in our own building(s)?
Storage solutions must be acquired and installed by facilities and must comply with all security requirements and building codes. Do not install anything in or on a building without proper approval.

Can I leave a GPS bike computer (e.g. a Garmin) attached to my bike in the rack?
Yes. A bike computer may remain on the bike in the rack or may be removed and stored in one of the designated, approved storage locations. (Note: It is against laboratory policy to store a bike inside a building.)

APPLICABILITY

Are any mobile devices exempt from this requirement?

- Authorized mobile devices assigned to protective forces and internal emergency services personnel (e.g., fire, medical, nuclear), whose primary responsibility requires the tactical response to emergencies within Secure Space and who have no other secondary means of communication, are exempt from the requirement. Mobile devices assigned to emergency personnel must remain powered off until required as a secondary means of communication.
- Nothing in the directive alters or supersedes legal or policy requirements regarding accommodation of employees' medical needs which continues to follow the Essential Job Function process. A cross-functional team is assessing current policies and processes.
- Controlled articles *which do not meet the definition of 'mobile device*,' and are registered and approved through the Controlled Articles Registration Process (CARP) site (i.e. laboratory testing equipment, cameras), are exempt from the requirement.

Do these requirements apply to SCIF's or Vault Type Rooms?
No, these high security areas have separate requirements in place that already prohibit mobile devices within these areas.

REPORTING

What happens if I bring a mobile device into a Secure Space once it is activated?
Before February 1, 2021: Mobile devices brought into Secure Spaces must be self-reported through the SIMP self-reporting tool at SIMP.sandia.gov and will be categorized as a Non-Incident/Non-Compliance (NINC), unless exposure to classified conversations occurs, which could result in an Incident of Security Concern (IOSC). This is the current process for personally owned mobile devices but will also include Sandia owned mobile devices effective when Phase 2 is implemented in November 2020.
Starting **February 1, 2021**: *Any* mobile devices brought into a Secure Space must be self-reported through the SIMP self-reporting tool at SIMP.sandia.gov and will be categorized as a Category B IOSC, at minimum.

How Do I Report?
Members of the Workforce with SRN computer access—go to SIMP.sandia.gov to access the Mobile Devices Self-Reporting Tool. Members of the Workforce without SRN computer access, or to report on behalf of another person—call 321 from a Sandia landline phone or (505) 845-1321 from a non-Sandia phone.

If my work area is in Secure Space, how can I stay connected to family members without a mobile device?
You are encouraged to ensure that your office desk phone number is included in your list of emergency contacts for family members, day care centers and/or schools. You may also access personal email via Chrome on the SRN. Additionally, the use of one-way pagers will be permitted inside Secure Space.

For more information about ACD 470.6, visit PEDs.sandia.gov.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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-NA0003525.

Advanced Change Directive (ACD) 470.6 – *Frequently Asked Questions*

Phase 1

PEDs.sandia.gov

What is ACD 470.6?

Advanced Change Directive (ACD) 470.6 is NNSA's implementation plan for the Committee for National Security Systems (CNSS) Instruction 510. ACD 470.6 was signed July 15, 2019 and governs the use of mobile devices within 'Secure Spaces' as defined by the federal requirement.

What is the requirement?

Each DOE site overseen by NNSA must assess its site facilities, identify all 'Secure Space' according to the ACD 470.6 definition, and develop its own implementation plan to comply with the directive by removing mobile devices (smart watches, tablets, personal and government issued mobile phones) from the identified spaces.

How do other NNSA sites currently manage mobile devices?

Sandia and Lawrence Livermore are the only sites in the complex that allow mobile devices into limited areas. All NNSA sites are implementing ACD 470.6.

What are the top 5 challenges for Sandia in implementing ACD 470.6?

- Sandia is one of the largest National Security Enterprise complexes with hundreds of buildings across 7 states.
- Implementation across all sites will require significant infrastructure resources, including a sharp increase in cell phone storage capacity.
- Mobile devices are an integral part of work efficiency at Sandia.
- Personal connectivity is a major component of work-life balance, and therefore an important consideration for employee satisfaction and retention.

Who is responsible for implementing the requirement?

Implementation planning and execution will be a coordinated through cross-functional teams including experts from Safeguards & Security, Facilities & Emergency Management, Infrastructure Services, CIO & IT Services and Environment, Safety & Health.

What is a mobile device?

A mobile device is a portable computing device that:

- can easily be carried by a single individual
- is designed to operate without a physical connection (e.g., wirelessly transmit or receive information)
- possesses local, non-removable data storage
- is powered-on for extended periods of time with a self-contained power source

Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, smart watches, tablets, and E-readers.

What is the difference between 'mobile devices' and 'portable electronic devices'?
ACD 470.6 uses the term 'mobile device' as defined above. The term 'mobile device' is a subset of the Sandia term 'portable electronic device,' which includes mobile devices (devices with data processing or transmitting/receiving capabilities) and storage devices (devices with storage capability, but no ability to process or transmit/receive information). Only mobile devices are impacted by ACD 470.6 requirements.

Does the requirement affect Sandia issued or government issued laptop computers?
No, the directive specifically states that it does not apply to government laptop computers that meet security requirements.

Does the requirement affect Virgin Pulse GoZone pedometers?
No, GoZone pedometers are not impacted. MOW may order GoZone pedometers through Virgin Pulse (you must create an account to enroll in Virgin Pulse; see 'Devices & Apps' link in Virgin Pulse profile to order).

What is the projected implementation timeline?
Phase 1: Completed January 1, 2020

- Removed personally owned mobile devices from all limited area buildings
- Sandia owned devices follow current policies

Phase 2: Implementation deadline January 31, 2021; Sandia leadership may elect to implement earlier

- Characterize all SNL buildings within limited areas to identify 'Secure Space'
- All mobile devices (personal and government) will be prohibited in area identified as 'Secure Space.'

Phase 3: Consolidate

- Consolidate classified processing within buildings where feasible to further refine the 'Secure Space' footprint.

Are Sandia-owned iPhones or iPads impacted in Phase 1?
No, Sandia-owned devices are not impacted in Phase 1; they continue to follow current polices. They will, however, be impacted in Phase 2.

What happens if I bring a personally owned mobile device into a limited area building (with the exception of designated, approved storage areas) between January 1, 2020 and the implementation of Phase 2?
Submit a report using the self-report tool at SIMP.sandia.gov. *Provided that the personal mobile device did not come into proximity with any classified discussions or processing, and did not enter a VTR or SCIF*, the event will be recorded as a non-incident, non-compliance (NINCs), which is a violation of corporate policy. If any of the above occurred, the event will be reported as a Category A or Category B incident.

What happens if I bring a mobile device into a Secure Space once it is identified?
Submit a report using the self-report tool at SIMP.sandia.gov. The event will be reported as a Category A or Category B incident.

Do the eligibility requirements still apply for bringing a personally owned mobile device into a limited area?
No, the former Rules of Use (PEDS100), including the eligibility requirements, are no longer in effect. Per the revised policy, all MOW, including cleared, uncleared and Foreign Nationals, are subject to the same requirements and restrictions regarding possession and use of personally owned mobile devices.

If I don't currently have a Sandia owned cell phone, may I request one?
The policies that govern the acquisition and use of Sandia mobile devices are being reviewed and updated in anticipation of increased usage and requests. Sandia cell phones require a business need.

May I use my Sandia owned cell phone for personal texts and/or calls?
Incidental personal use of Sandia IT equipment is allowed but the personal use must be consistent with the requirements identified in IT002, Use Sandia's Information Technology Resources Policy.

What can I do to prepare?

- Update emergency contact information by providing Sandia mobile and/or desk phone numbers to family, friends, schools, child care centers, etc.
- Updated contact information through the HR Self Service site > Personal Details > Emergency Alerts to ensure that alerts will be sent to Sandia devices.
- Consider adjusting commuting routines to allow for safe storage of personal cell phones and other devices, especially during the initial weeks of implementation.

Where can I store my personally owned mobile device prior to the implementation of Phase 2?

You may store mobile devices in your vehicle, at limited area entry turnstiles, or in the following designated, approved storage locations at limited area building entrances (list also available at PEDs.sandia.gov). Locations will be marked with signage.

701: Northeast entrance and northwest entrance
800/801: Main entrance of Bldg. 800 Property Protection Area (PPA)
810: Main lobby
822: Main entrance (personal phones may traverse through the 822 breezeway, but may not enter building 821)
880: North vestibules B and D
887: Northwest entrance lobby and southwest entrance vestibule
898: Main lobby entrance in the PPA
960: Main lobby (west side of building)
962: Main lobby
6577 (TA-V): Main lobby
6585 (TA-V): Main lobby
910 (CA): 1st floor main lobby
915 (CA): PPA café wing

- Designated, approved storage locations meet all ACD 470.6 requirements for non-Secure Space.
- Storage areas will be marked with signage.
- Inside a limited area, mobile devices may be stored in ***these buildings only, and only within the designated storage areas***.
- Current external storage boxes may be used. ***Keys to storage boxes may not be kept overnight.***
- Devices may not enter, or be carried through, any other part of the identified buildings, or any limited area building not approved.
- No classified discussions are allowed in the storage areas.
- Since storage will only be available in designated, approved locations, consider leaving personally owned mobile devices at home or in your vehicle.
- Like luggage at the airport, many phones look alike. Consider making your device easily identifiable. And when you leave, make sure you take your own, not someone else's!

Click here for a map of current mobile device storage locations at SNL/NM.
Click here for a map of current mobile device storage locations at SNL/CA.

My building is divided by a limited area boundary; part of the building is a limited area, and part of the building is a Property Protection Areas (PPA) or General Access Areas (GAA). Are mobile devices permitted in the PPA/GAA portion of the building?

Yes.

May I use existing storage boxes located in Property Protection Areas (PPA) or General Access Areas (GAA) that are adjacent (connected) to limited areas, even if they are in the same building (as described above)?

Yes, during Phase 2, existing storage located in PPAs or GAAs adjacent to limited areas may be used to store mobile devices. As 'Secure Space' and 'Non-secure Space' is identified, existing storage will be evaluated and relocated if it does not meet all requirements in the directive.

I ride a bike, a bus, or a carpool to work and therefore will not have the option to store my personally owned device in my vehicle. Will there be enough storage?
The project team recognizes the importance of this concern and is working toward permanent solutions that will provide plenty of storage to support all types of commuting alternatives.

If I have a handicapped placard or other permit that allows me to park inside the Limited Ares, will I be allowed to store my phone in my car (inside the limited area)?
Yes. A mobile device may be stored in any vehicle that is authorized to park within a limited area.

How does the workforce feel about allowing mobile devices into limited areas?
A Counterintelligence survey spanning the past 12 months posed the question: “Do you believe the benefits of allowing PEDs into the limited areas outweigh the risks?” Out of 16,135 respondents:

41% - Yes
59% - No

Is theft of mobile devices from storage areas expected to be a problem?
Sandia has no recorded reports of stolen mobile devices within limited areas.

If I am escorting an uncleared individual into a limited area, am I still required to brief them about controlled and prohibited articles?
Yes, escorts should still brief uncleared individuals prior to entering a limited area:

- Ensure no unauthorized (prohibited) articles enter a limited area.
- Ensure Bluetooth and WiFi are turned off on any mobile devices—personally owned or Sandia owned.
- Ensure that the individual is prepared to store any personally owned mobile devices in their possession in a designated, approved storage location.

For more information about ACD 470.6, visit PEDs.sandia.gov.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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-NA0003525.