SA 2712-CVC # (10-2002)
Supersedes (3-2002) issue

Sandia National Laboratories

CONTRACTOR/VISITOR - COMPUTERS
TEMPORARY, ONE-TIME EXCEPTION TO SNL POLICY

Complete this form to take Computers into Sandia premises (both Limited Areas and Property Protection Areas (PPAs)).
This form may also be used to obtain authorization for potential TSE (technical surveillance equipment).
FAX the completed form (or send a copy) to the host's Center Computer Security Representative (CSR) BEFORE going on-site.
Register in NWIS for any one of these conditions: network connections; or multiple visits; or for stays exceeding one month.

Visitor Name _____ Start Date _____
Visitor Business Affiliation _____ End Date _____
SNL Host Name _____ Phone _____
Center's CSR's Name _____ CSR FAX (or mail stop) _____
Equipment Description _____
Business Reason for bringing equipment on-site _____
Location(s) where equipment will be taken/used _____

Equipment Identification	Peripheral Equipment (if any)
Model _____	Model _____
Make _____	Make _____
Identifying Number	Identifying Number

Are you a Foreign National? ☐ YES ☐ NO If YES, the approved FNR number is _____

This equipment is owned by *(Check **only one**)*

☐ US Government Owned ☐ Business Owned ☐ Personally Owned

If any questions below are answered "YES", Technical Surveillance Countermeasures (TSCM) review may by required. *(See reverse side)*

Activated Audio Recording Capability? (e.g. microphone) ☐ YES ☐ NO
Activated Video Recording Capability? (e.g. camera) ☐ YES ☐ NO

If any questions below are answered "YES", then additional actions apply.

Will you connect to the unclassified network? ☐ YES ☐ NO If "YES", perform a virus scan, register in NWIS and *(See reverse side)*.
Is there any classified equipment involved? ☐ YES ☐ NO If "YES", contact your CSR/NSO.

Activated RF wireless networking? **NO** NNSA(DOE)/AL approval required. Begin approval process by completing RF-Proposal form.

Rules-of-Use

Minimum Requirements

- **Don't connect this equipment to a network without first obtaining approval.**
  Computers requiring connection to a Sandia National Laboratories network(s) must perform a virus scan with current signatures, register in NWIS, obtain a WebCARs authorization, complete a network action request and obtain approvals prior to connection.
- **Any equipment brought onto Sandia National Laboratories Sites is subject to monitoring and or inspection.**
- **No other equipment may be substituted under this authorization.**
- **This completed form must remain with the equipment at all times while on a Sandia National Laboratories site.**
- **FAX the completed form (or send a copy) to the host's Center Computer Security Representative (CSR) BEFORE going on-site.**
- **A copy of the completed form must be retained in the host Center/Department for 3 months following the visit.**

Additional Requirements for Limited Areas

- Portable electronic devices must be in possession of the visitor at all times when in a limited area.
- No activated RF wireless networking capability is allowed. DOE would have to approve an exception.
- TSCM must review, prior to use, audio recording or video recording devices.
- The equipment will not be taken into any classified facility that contains SCI, SAPs, or TS without the approval of the facility security officer.

Additional Requirements for Classified Devices

- A copy of the 'home site' accredited Computer Security Plan for the device must remain with the device.
- This device will be only operated as a standalone and will NOT be connected to a Sandia resource.
- Any unclassified media inserted into a Sandia classified device that has the capability of writing to the media must be appropriately marked, stored and transported. The media can only be transported as classified media. (This is true whether the media is written to or not.)

I have reviewed the form for completeness and accuracy and accept responsibility for authorizing this equipment onto a Sandia National Laboratories site.	SNL Host Signature *(required)*
The information on this form is accurate and I accept the above Rules-Of-Use	Visitor Signature *(required)*

Security review(s) signatures *(if required)* _____
(please identify type of review – computer security / TSCM / facility security officer)

Completion of this form permits an exception to CPR 400.2.13.10.
Security Officers: Please ensure that all information is completed.

Instructions for completing the form.

1. Complete the front side of this form. Sign it. Obtain SNL Host signature.

2. Determine basic approval requirements and obtain necessary signatures.

Basic required approvals
Contractor/Visitor Companies

		US Citizen		
	Foreign National Approved FNR required	**US Government Owned**	**Business Owned**	**Personally Owned**
Property Protected Area	Approved FNR Host approval	No approval required unless networked	Host approval	Host approval
Limited Area Notify Computer Security if classified is involved	Approved FNR Host approval Computer Security review in CA	No approval required unless networked or if classified is involved	Host approval	Host approval Computer Security concurrence

Hosts must be Sandia National Lab employees.

Duration of visit

No additional authorization is required for on-site access up to:
- 1 week for personally-owned equipment
- 1 month for company-owned equipment

For visits of less than 1 month involving US government owned equipment this form is not required.

Access exceeding the above timeframes must follow the standard procedures including NWIS registration.

Foreign Nationals
Approved FNR

Network Connections
Virus scan with current virus/Trojan signatures, Approved WebCARs application, NWIS registration network action request.

3. Determine **if the following additional reviews/approvals are required**

Personally-owned equipment to be taken into a Limited Area
Computer Security Review - REQUIRED

Activated Audio Recording or Video Recording Device
TSCM Review - REQUIRED

Accessing SCI, SAPs, or TS Facility
Approval of Responsible Facility Security Officer -REQUIRED

4. **Once the form is completed and the required approvals are obtained, FAX/send the front of this form to the host's Center Computer Security Representative before going on-site.**