(User Name) (Token#)

Print Form

U.S. Department of Commerce (DOC)/NOAA/OAR/ESRL-GSD
High Performance Computer System Remote Access User Security Agreement

Purpose and Scope: I understand I am being granted permission, for one (1) year, from the signatory date, renewable annually, for use of ESRL Remote Access Services which allow for access, both remotely and locally to NOAA/GSD IT systems and that my use of this access may be monitored by DOC for compliance with this policy. I understand that for some remote access and other services, I will need to take possession of a Safeword Token device. I understand this access may be allowed in conjunction with a separately approved request for Flexiplace (teleworking). I have completed the NOAA IT security training within the last 12 months, and I hereby attest that I have read and understand the **DOC Unclassified System Remote Access Security Policy and the DOC Remote Access Procedures Policy located under References at:** (*https://security.esrl.noaa.gov/*). I understand that all data distribution from the NOAA/GSD Supercomputer, for other than authorized use, is strictly prohibited, and that all rules and restrictions must be followed regarding proprietary data available on GSD computers. In particular, proprietary data cannot be copied from GSD computers without permission.
See http://rdhpcs.noaa.gov/boulder/user_info.html#restricted_datasets for more information on restricted databases.
I agree to comply with these policies, and I understand that my failure to comply with these policies may result in termination of my remote access privileges and/or legal action. Please fill in all required user information areas.

Section 1: Remote Access Precautions:

Protection of Data: I hereby affirm and acknowledge my responsibility to ensure the confidentiality, integrity, and availability of all forms of Government information in accordance with DOC IT Security Policy and the DOC Security Manual, in a manner consistent with its sensitivity. I accept my responsibility to provide reasonable physical security for all NOAA resources. I agree to implement and maintain, as directed, the following mandatory countermeasures on equipment used to process NOAA information:

1. Encrypt authentication credentials.
2. Never use public-access equipment for Tier 2 or 3 access.
3. Configure computers to not "remember" NOAA passwords.
4. Remote access users will maintain hardware and software as required.
5. Anti-virus software is required on all equipment connecting to NOAA resources.
6. Install and use password-protected screensavers when idle for 15 minutes or more.
7. Agree to comply with regularly scheduled maintenance requirements for NOAA resources.
8. Use a provided mechanism for encrypting sessions that meets at a minimum AES or Triple-DES.
9. Install and update (at least monthly) security related patches on personally owned devices that can be patched.
10. Never configure remote access computers as servers (e.g., web servers, private e-mail servers, File Transfer Protocol (ftp)).
11. Clear browser history and cache and close browser when finished with remote access needs for personally owned equipment.
12. Do not share or reveal NOAA usernames and passwords to anyone (including family members) to prevent unauthorized access to NOAA IT systems and data.
13. Install and configure to automatically update (at least bi-monthly), and run anti-virus software on personally owned equipment used for remote access.
14. Do not save Government information and applications to the hard drive of the remote access computer (applies to publicly accessed equipment only).
15. A personal firewall is required on government-owned equipment and on personally owned equipment when broadband technologies are used.
16. Authenticate first to a remote access gateway on the NOAA network perimeter as well as comply with the information system owner's requirements for authentication and identification of the specific internal system or data resource being accessed.
17. Maintain proper configuration of direct-access software, to include that no remote control/direct access software may be permitted to use dial-up connectivity unless transmissions are encrypted in accordance with the standards of the DOC Remote Access Policy.

Access Requested:

SSH To Supercomputer (HPCS Project Name) (Justification)

Protection and Maintenance of Equipment (Check all that apply):

☐ In the case of local and remote access via government-owned equipment, I will not alter the configuration of government equipment unless authorized in writing to do so. I will protect DOC-owned/ furnished resources and submit the equipment for periodic maintenance as required by DOC.

☐ In the case of local and remote access via equipment owned by another organization, I will verify with that organization that suitable anti-virus software and firewalls are implemented. The organization is responsible for periodic software and security maintenance.

☐ In the case of remote access via personally-owned equipment, I will provide information about connectivity and security software configured on my personally-owned equipment. DOC/NOAA/GSD authorizes me to use my personally-owned computer for remote access and is not required to install or support maintenance of the hardware or personally-owned software. I will install and maintain the following (required for SSH access):

AntiVirus Software	Firewall Software	Specify Other
Select One	Select One	

Computer Incidents (remote access): I also acknowledge the possibility, however small, that sensitive information could potentially be viewed or downloaded by others than myself as a result of my remote access. I fully understand that it is my duty to exercise due care in protecting this information and to immediately report any unauthorized disclosure or compromise to my supervisor and to the ESRL ITSO so that appropriate procedures may be initiated. I further understand that, after proper coordination with law enforcement authorities, the Government may temporarily seize the device used to gain remote access for the purposes of forensic examination and sanitizing of compromised information. Additionally, during this process I understand there exists a risk that system files and programs may be erased or damaged, or that unintentional damage may occur to the computer hard drive. I hereby waive any and all claims against GSD,ESRL, NOAA, the Department of Commerce, the Federal Government, and individual officers, employees, agents and contractors thereof, arising out of necessary security procedures and actions with respect to personally-owned IT equipment and any such damage to, or erasures of personal data.

Section 2: User Information: User Name:

_____
(First Name) (Middle Initial) (Last Name)

Are You a United States Citizen? ☐ YES ☐ No **(If No, Complete Section 3 of this form.)**

_____ _____
(User's Organization Information) (Address: Street, City, State, Country ZIP)

_____
(Address Cont:) (E-Mail Address and Phone#)

User Affiliation: ☐ Contractor ☐ CIRA ☐ CIRES ☐ Collaborator ☐ Federal ☐ Intern

Other, Explain: _____

Section 3: Foreign National Information:

Country of Birth: _____ Current Citizenship: _____

Country of "Permanent Residence": _____

Please Indicate the Type or Types of Credentials You Posses:

☐ Passport ☐ Green Card ☐ Visa Select Visa Type (Nonimmigrant) Other _____

I have read, and agree to comply with, the DOC IT Security policies for remote access and the other conditions of this form, outlined under the Purpose and Scope, and Section 1 above.

_____
(Signature) *(Date)*

Section 4: Approvals:

HPCS Management Team Lead (Leslie Hart) _____
(*Signature*) (*Date*)

ESRL ITSO/GSD ITSO: _____
(*Signature*) (*Date*)

☐ **Completed Security Awareness Training Course** _____
(Completion Date) (Certificate #)

Token Information:

_____ _____ _____ _____ _____
(Token #) (Issued By) (Date) (User Name) (Token Groups)

Annual Review: To be verified by Division IT management, ITSO and Signed by HPCS Manager

Account Active No Changes	Sec Training Comp. Date	New Certificate #	HPCS Manager