U.S. Department of Commerce (DOC)/NOAA/GFDL
Unclassified System Remote Access User Security Agreement

Purpose and Scope: I, _____, understand I am being granted permission
(print name)
to remotely access the unclassified DOC IT systems as specified below, and that my use of this access may be monitored by DOC for compliance with this policy. This agreement will be renewed annually. I understand this remote access may be allowed in conjunction with a separate approved request for teleworking. I have completed DOC IT security training within the last 12 months, and I hereby attest that I have read and understand the NOAA/GFDL Computer Use Policies for remote access and password management. 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 disciplinary action. GFDL will notify users of changes to these policies.

Users who do not remotely access GFDL via their CRYPTOCard token card for 90 days may temporarily have their remote access account suspended until they call operations (609-452-6560) or e-mail oar.gfdl.help@noaa.gov requesting to have their account reactivated.

Remote access of the following types is requested (**circle Y**) / not requested (**circle N**) for official use:

Access Method:		Select system(s):	
Y/N	SSH	**Y/N**	Scientific Systems (Linux Workstations, Supercomputer, Scientific Windows System)
Y/N	Call-back Modem	**Y/N**	Administrative Systems

Do you need System Administration Access? **Y/N** If '**Y**' list all systems: _____

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.

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

☐ In the case of remote access via GFDL-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. Check this box if you think you may ever want to borrow one of GFDL's loaner systems.

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

☐ In the case of remote access via personally-owned equipment, the government may provide software installation disks and support software used to process DOC/NOAA information as permitted by software license agreements. I will abide by the license agreements for DOC-furnished software. DOC/NOAA/GFDL authorizes me to use my personally-owned computer for remote access, and although NOAA/GFDL may provide limited support, it is not required to support maintenance of the hardware or personally-owned software.

Check one: I ☐ will / ☐ will not be accessing unclassified DOC IT systems via a broadband (e.g.: DSL, cable-modem) connection.

I will install and maintain the following:

Anti-virus software (required for **all** access)
☐ McAfee (Available @ https://www.csp.noaa.gov/noaa/antivirus/index.html)
☐ Other _____ (specify vendor and version)

Personal firewall _____ (specify vendor, model number/version)
(Required for **broadband** access only, recommended for **all** access)

Computer Incidents: I also acknowledge the possibility, however small, that Government 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 an unauthorized disclosure or compromise to my supervisor, to *oar.gfdl.itso@noaa.gov* (GFDL ITSSO), and to *ncirt@noaa.gov* 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.

Remote User's Signature _____ Date _____

Submit this form to your supervisor, contract monitor, or the head of your research group. Remote collaborators should send this form to your local GFDL sponsor for completion.

I hereby certify that this (check one) ☐ federal employee/ ☐ contractor/ ☐ collaborator requires remote access as described herein to accomplish the DOC mission:

Supervisor / COTR / Group Head Printed Name _____ Signature _____ Date _____

Submit completed forms to Bob White (Room 162) or Jeff Flick (Room 165).

Verification and Approval:

☐ Completed IT Security Awareness Course

Confirmed By (GFDL ITSSO) _____ Date _____

☐ Approved ☐ Disapproved

Director / Senior IT Manager Signature _____ Date _____

For Official Use Only:

CryptoCard Serial No. _____ Issued by _____ Date _____

Remote Access Username _____ *User ID* _____ *Bin No.* _____ *GFDL Project (Group)* _____