ARM Data System
Visitor PC and Instrument
Network Connection Policy

1. The following are eligible to attach a personal computer or instrument to the visitor network at any of the ARM CART sites provided there is a valid reason for the connection:
   - Any member of the ARM Science Team.
   - Any member of ARM Infrastructure, Engineering, Operations, or
   - Quality Control group.
   - CART Site IOP visitors; and
   - Personnel with visiting or development instruments at the ARM CART site.

2. Applicants must complete an application form and have it approved by ARM Data Systems Operations (The ARM SAR process).

3. The connection is for the purpose of analysis or research related CART site measurements or instrumentation or to conduct business related network activities (e-mail, etc) while visiting the site.

4. The primary mechanism to acquire data from ARM CART measurement systems is through the ARM Archive (www.archive.arm.gov). Users requiring access to data streams which are not shipped to the archive may request an account on the CART site R1 system to acquire such data.

5. Remote access to any CART site network is via significantly limited and expensive Internet bandwidth - especially to the NSA and TWP sites. This bandwidth is primarily for transfer of ARM data to the ARM DMF and Archive. Users are expected to not abuse the privilege of remote access by excessive, heavy use of the connection.

6. By default, access to the system from off-site is restricted to ssh (or sftp, scp) protocol version 2 only. If there are additional remote access requirements provide them below. Protocols which use non-encrypted authentication (ftp, telnet, etc) are discouraged.

7. At the present time, access to the internet from the connected system is not restricted.

8. SDS Operations staff will, periodically scan attached visitor systems for network vulnerabilities. System owners will be notified of any vulnerabilities found. Depending upon the level of risk of the vulnerability (as judged by SDS Operations staff) access to the system may be restricted or the system removed from the network.

9. SDS Operations staff may monitor traffic addressed to and generated by visitor systems. There should be no expectation of privacy. Any evidence of inappropriate network usage, abuse of network bandwidth, or activity which threatens the integrity of the network or other systems will result in removal of the system from the network.

10. Systems should meet the following requirements:
    - Windows systems should have anti-virus software installed and updated with current signatures;
    - Systems should have the latest vendor recommended security patches installed;
    - Systems shall have any un-necessary services turned off (ftp, telnet, PCAnyWhere, http, etc).

I affirm that I have read and understand the ARM Data System Visitor PC and Instrument Network Connection Policy and I agree to operate within and adhere to the stated requirements within the policy.

______________________________ ____________________________________

Printed Name Signature

____

Date