



TeraGrid User Responsibility Form

Last updated 3/7/2008 (v1.9)

1 Introduction

The TeraGrid computing facilities (which include its hardware, software, network connections, and data) are a vital but limited resource for the scientific community. Therefore the TeraGrid sites have an obligation to protect those facilities and ensure they are used properly. Additionally, sites have legal and other obligations to protect resources and the intellectual property of the users.

Because we cannot do this job alone, we depend on your cooperation. Responsible conduct on your part helps ensure that the maximum amount of CPU time is available to you and other researchers.

Failure to use these resources properly may result in various penalties, including civil and criminal action.

Your signature on this form implies that you have read and understand your responsibilities stated here. If you have any questions about this document, please use the contact(s) identified in §6.1 to discuss the issues. Otherwise, sign and return this form to enable/continue use of your account.

NOTE: *The last page of this form must be signed, and mailed or faxed to the TeraGrid Allocations Department within 30 days. If the form is not returned within 30 days, your TeraGrid account will be deactivated.*

2 Requirements

2.1 Individual Account Management

You have responsibilities to protect your account from unauthorized use. Tools are provided to help provide this protection, but you are responsible for using these tools properly.

2.1.1 No Sharing Accounts

An account is for one user only. It is not to be shared with others; neither students nor

other collaborators. User certificates are not to be shared either.

2.1.2 Protecting Passwords

Passwords and certificates are the keys to account access. You are responsible for protecting your passwords and certificates. Protection includes not sharing passwords, not writing passwords down where they can be easily found, and not using tools which expose passwords on the network (e.g. telnet). See the Guidelines section (§5) for more information.

The private key portion of a certificate is the equivalent of a password. You are responsible for ensuring that file and directory permissions prevent others from reading or copying any private keys.

2.1.3 Authorized/Acceptable Use

Access is not authorization. Having an account does not confer upon you the right to do anything that you are capable of with that account.

2.1.3.1 Authorized Use

Your account is granted for the activity stated on your application. Your use of the account should be limited to that activity.

2.1.3.2 Acceptable Behavior

The following activities are explicitly considered unacceptable and are subject to the penalties outlined below:

- using, or attempting to use, TeraGrid computing resources without authorization or for purposes other than those stated on your application for computer time
- tampering with or obstructing the operation of the facilities
- reading, changing, distributing, or copying others' data or software without authorization
- using TeraGrid resources to attempt to gain unauthorized access to other (non-TeraGrid) sites
- activities in violation of local or federal law

2.1.4 Reporting Suspicious Activity

You are responsible for reporting, as soon as possible, suspicious activity on your account, or exposure or compromise of passwords, passphrases, or certificates. See section (5) for reporting procedures.

2.2 Community Account Management

NSF centers also support community accounts, where users can login to a portal or other front-end and execute jobs via a single username on the back end. Because risks may be greater and usage patterns less certain for these types of accounts, additional information

is required to help prevent security incidents. This information must be submitted before jobs can be run externally via community accounts. Additionally, TeraGrid Resource Providers may choose to impose their own limitations on community accounts through operating system tools, restricted shells or other means.

Because the gateway maintains control of these allocations, the gateway PI must ensure that NSF computational resources are used in a manner consistent with the award and that reasonable attempts have been made and tools installed to ensure appropriate usage. This includes monitoring of all gateway usage by the community.

2.2.1 Additional required information for community accounts

- IP address or DNS name of the portal machine
- Logging of requester's IP address, UTC timestamp and username on the portal
- Current estimated long-term disk storage requirements for the community account (this can be modified in the future to accommodate gateway growth)
- Paths to directories on the RP cluster where scripts and executables can be run by an un-verified user from the portal, e.g. \$HOME/bin
- Optionally, for each script or executable in the named directory, provide
 - Estimated maximum number of processors/nodes
 - Estimated maximum run time
 - Estimated short-term storage requirements per user per job

This information must be provided with all community account requests. To request a community account, login to the <https://portal.teragrid.org>, then click on 'My TeraGrid' and the 'Community Account' subtab.

2.3 Data Confidentiality

It is your responsibility to ensure the confidentiality of any intellectual property or other confidential data used on TeraGrid resources.

TeraGrid sites provide technology to preserve the confidentiality of data, but it is your responsibility to use that technology appropriately.

2.3.1 Confidential Data

Some of your data may not be considered intellectual property but may have confidentiality requirements. It is your responsibility to be aware of those requirements and verify whether or not a given TeraGrid site has the capabilities appropriate to the level of protection required.

2.3.1.1 Proprietary Data

Proprietary or private data (which may also be considered intellectual property) may have confidentiality requirements imposed by the owner of the data.

2.3.1.2 "Regulated" Data

Some data may not be explicitly confidential but may have a confidentiality requirement due to various laws or organizational policies. Some examples might be:

- medical records
- student records
- personal identifying information (e.g. Social Security numbers)

It is your responsibility to be aware of those requirements and verify that a given TeraGrid site can provide appropriate protection. Also be aware that some sites may be subject to state laws which impose requirements on any data stored on those sites.

2.3.1.3 Sensitive but Unclassified Data

Some types of data or resources may be considered "Sensitive but Unclassified" by the Federal government, and thus may have restrictions and protection requirements.

It is your responsibility to be aware of those requirements and verify that a given TeraGrid site can provide appropriate protection.

2.3.1.4 Intellectual Property

You have specific responsibilities with regard to intellectual property used on TeraGrid resources

2.3.1.5 Acknowledgment

Papers, publications, and web pages of any material, whether copyrighted or not, based on or developed under TeraGrid-supported projects must acknowledge this support by including the following paragraph:

"This material is based upon work supported by the National Science Foundation under the following NSF programs: Partnerships for Advanced Computational Infrastructure, Distributed Terascale Facility (DTF) and Terascale Extensions: Enhancements to the Extensible Terascale Facility."

In addition, a copy of each publication must be emailed to allocations@teragrid.org. More information on publications can be found at <http://www.ci-partnership.org/Allocations/acknowledgment.html>.

2.3.1.6 Software Development

Software developed with allocations approved by NSF, or by proxy, via the allocations processes governing allocation of TeraGrid resources, is subject to the NSF General Grant Conditions (GC-1) and thus certain copyright restrictions apply. In the July 2002 revision of this (http://www.nsf.gov/awards/managing/general_conditions.jsp?org=NSF), this issue is specifically addressed in Article 18. Copyrightable Material.

2.3.1.7 Publication

Work performed under a peer-reviewed allocation must be published in the open literature.

2.3.1.8 Non-Academic User Requirements

Non-academic (corporate/industrial, government, etc.) users frequently have more stringent usage requirements than those that might be provided by the TeraGrid as a whole or by a particular site within the TeraGrid. It is the user's responsibility to assure the resources used satisfy the requirements of their organization.

Also see 2.3.1.3 above.

2.4 Software Licenses

All software used on TeraGrid systems must be appropriately acquired and used according to the specified licensing. Possession or use of illegally copied software is prohibited. Likewise users shall not copy copyrighted software or materials, except as permitted by the owner or the copyright. Some software installed on TeraGrid resources may require special authorization in order to be used. Users must abide by the requirements for protecting it from misuse.

2.5 Final Reports

Requests for subsequent allocation awards will not be allowed until an end of project report has been received for all prior awards. It is recommended that renewals and continuing projects also include a copy of prior award final reports as an attachment to the submitted proposal. Details on end of project reports are available in the posted PACI Allocation Policies at: <http://www.paci.org/SummaryProjectReport.html>.

2.6 Additional Requirements

Individual sites may be subject to state/local laws and/or have organizational policies with additional requirements beyond this policy.

Those organizations will make those policies available. It is your responsibility to be aware of and abide by those policies.

3 Penalties

Failure to abide by this agreement may result in a variety of penalties imposed.

3.1 Account Suspension/Revocation

Accounts may be temporarily suspended or permanently revoked if compromised or abused.

Your account may be suspended without advance notice if there is suspicion of account compromise, system compromise, or malicious or illegal activity.

3.2 Loss of Allocation

This policy can result in loss of your current allocation and possibly the inability to obtain future allocations.

3.3 Administrative Action

Abusive activity may be reported to your home institution for administrative review and action.

3.4 Civil Penalties

Civil remedies may be pursued to recoup costs incurred from unauthorized use of resources or incident response due to compromise or malicious activity.

3.5 Criminal Penalties

Activities in violation of federal, state, or local law may be reported to the appropriate authorities for investigation and prosecution.

4 Disclaimers

4.1 Additional requirements

As stated in §2.6, individual TeraGrid sites may be subject to requirements beyond the scope of this document.

4.2 Support/Diagnostic Access

Authorized TeraGrid site personnel may review files for the purposes of aiding an individual or providing diagnostic investigation for TeraGrid systems.

4.3 Monitoring

User activity may be monitored as allowed under policy and law for the protection of data and resources.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site or law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such at the discretion of authorized site personnel.

4.4 Access Notification

Access to user data and communications will not normally be performed without explicit authorization and/or advance notice unless exigent circumstances exist. Post-incident

notification will be provided in such cases.

5 Guidelines

The following are suggestions for helping maintain the security of your account.

5.1 Password Management

- Do not write down your password where it can be easily found and/or associated with your account.
- Do not tell anyone your password, not even TeraGrid support staff. Support staff will never need your password, will never ask for it, and will never send a password in e-mail, set them to a requested string, or perform any other activity which could reveal a password.
- If someone insists they need your password to do something, report it to the TeraGrid helpdesk: <http://www.teragrid.org/links/helpdesk.html>.
- Do not store your password(s) in unencrypted files or even in encrypted files if possible.
- Pick passwords that are difficult to guess. Birthdays, family names, and single dictionary words are examples of easily guessed passwords.
- Change your password periodically, even if you have no reason to believe that anyone else has it.

5.2 Reporting Suspicious Activity

(See section (6) below for appropriate contacts)

5.2.1 Password Exposure

If you think your password may have been compromised or exposed, but have no reason to believe that your account has been used, change your password immediately.

5.2.2 Certificate Exposure

If you believe your certificate has been exposed, revoke your certificate and have a new one issued.

5.2.3 Account Compromise or Suspicious Activity

If you believe your account has been compromised or find signs of suspicious activity, take the following actions:

- notify the TeraGrid helpdesk immediately (<http://www.teragrid.org/links/helpdesk.html>)
- do not modify files found in your account
- do not execute unknown programs you might find
- if possible, do not use your account until the issue is resolved

Some indications of account compromise include:

- files in your home directory or project areas which you did not create
- alteration or deletion of your files not done by you
- discrepancies between your allocation balance and what you think you have used

6 Contacts

6.1 General Assistance

For general assistance in understanding this policy and how to fulfill your responsibilities under this policy, contact help@teragrid.org.

6.2 Suspicious Behavior

Suspicious activity, which may indicate an account or system compromise, should be reported to the TeraGrid helpdesk: <http://www.teragrid.org/links/helpdesk.html>.

6.3 Password and Certificate Changes

Contact help@teragrid.org for assistance in changing your password, passphrase, or revoking and issuing a new certificate.

6.4 Exposure of Passwords, Passphrases, etc.

Contact help@teragrid.org for assistance

See below for required return form

----- return only the last page -----

7 Acceptance Statement

The undersigned acknowledges that s/he has read the TeraGrid User Responsibility Form and understands that information. The undersigned also acknowledges that s/he will abide by the stated policies and procedures to the best of his/her ability. The undersigned is also under obligation to abide by any future changes to the TeraGrid User Responsibility Form. All users will be notified when changes are made to the TeraGrid User Responsibility Form. The current TeraGrid User Responsibility Form can also be found on the TeraGrid web site in both HTML (http://www.teragrid.org/userinfo/access/user_responsibility.html) and PDF (http://www.teragrid.org/userinfo/access/user_responsibility.pdf) formats.

This page must be returned **within 30 days** to the TeraGrid Allocations Department via fax or US Mail.

Send mail to:

TeraGrid Allocations
1008 NCSA MC 257
1205 W. Clark Street
Urbana, IL 61801

or fax to: +1-217-265-0524

Name: _____
Institution: _____
E-Mail: _____
Daytime Phone: _____
Academic status: _____
Signature: _____
Date: _____