



## TeraGrid User Responsibility Form

*Last updated 8/06/09 (v2.2.2)*

### Introduction

All TeraGrid resource provider (RP) sites have legal and other obligations to protect shared resources as well as the intellectual property of users. Users share this responsibility by observing the rules of acceptable use that are outlined in this document. TeraGrid resources include hardware, software, network connections, and storage. Each resource is finite and shared by the entire research community. Responsible conduct on the part of each user is essential to ensure equitable and secure access for all. Failure to use TeraGrid resources properly may result in the penalties outlined in section 5, including those imposed by TeraGrid, civil, and/or criminal penalties.

Each time an application for TeraGrid resources is submitted, the Acceptance Statement, or last page of this form, must be received by the TeraGrid Allocations Department within 30 days. If it is received in time, the account will be enabled or continued—if not, it will be deactivated. Your signature serves as acknowledgement that you have read and understand your responsibilities as a user. The Acceptance Statement should be sent via email, fax, or US mail to the TeraGrid Allocations Department, 1008 NCSA MC 257, 1205 W. Clark Street, Urbana, IL 61801. If you have questions, please write to [help@teragrid.org](mailto:help@teragrid.org).

### 1.0: Account, Password, and Certificate Management

TeraGrid will provide you with the accounts necessary to access allocated systems. An account is assigned for one user only and must not be shared with others—including students and/or collaborators. For community accounts, see section 1.2 below.

Passwords and certificates are the keys to your account. Never share a password out loud, or write it down where it could be found and/or associated with your account. Never use tools which openly expose them on the network, such as telnet. Make sure that file and directory permissions prevent others from reading or copying the private key portion of certificates, which is the equivalent of a password. Do not store your password(s) in unencrypted files or even in encrypted files if possible.

TeraGrid support staff will never ask for your password, and will never send a password via e-mail, set them to a requested string, or perform any other activity which could reveal it to others. If a TeraGrid support person insists that you share your password, report it to the TeraGrid helpdesk: [help@teragrid.org](mailto:help@teragrid.org).

#### 1.1: Create Effective Passwords—Change Them Periodically

Create passwords that are difficult to guess and that cannot be found in a dictionary. Birthdays, family names, and single words are examples of easily-guessed passwords. Change your password periodically, even if you have no reason to believe that anyone else has it.

## **1.2: Community Account Management**

National Science Foundation (NSF) centers support community accounts, where users can login to a portal or other interface and execute jobs via a single username on the back end. Because a TeraGrid gateway maintains control of allocations, the gateway authority monitors all usage to ensure that the resources are used in a manner that is consistent with the award. TeraGrid RP administrators may also choose to impose limitations on community accounts through operating system tools, restricted shells, or other means.

## **1.3: Account Compromise or Suspicious Activity**

TeraGrid provides tools that will help protect accounts from unauthorized use; however, it is your responsibility to use these tools properly. If you believe your account has been compromised or if you find signs of suspicious activity, take the following actions:

- notify the TeraGrid helpdesk immediately ([help@teragrid.org](mailto:help@teragrid.org))
- 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 that a compromise has occurred include:

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

## **2.0: Unauthorized Use and Access**

How you intend to use TeraGrid resources must be clearly defined in your allocation request. Subsequently, access is granted specifically for the research that is described in the request—nothing else. Just because you can access a resource does not mean that you have authorization to do so. You must operate within sanctioned parameters regardless of what may be technically possible.

## **3.0: Unacceptable Behavior**

Following are examples of unacceptable behavior which are subject to the penalties described in section 5.0:

- Using, or attempting to use, TeraGrid resources without authorization or for purposes other than those stated on your allocation request
- 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, state, or federal law

#### **4.0: Reporting Suspicious Activity**

You are responsible for immediately reporting exposed or compromised passwords, keys, passphrases, or certificates as well as suspicious activity on your account. Report all suspicious activity, whether or not you suspect an account or system has been compromised, to the TeraGrid help desk: [help@teragrid.org](mailto:help@teragrid.org).

#### **5.0: Penalties**

Failure to abide by this agreement may result in a variety of penalties, including:

- Temporary account suspension or permanent revocation without notice if there is suspicion of account or system compromise, malicious, or illegal activity.
- Loss of current allocation and the inability to obtain future allocations.
- Abusive activity may be reported to your home institution for administrative review and/or action.
- Civil litigation may be pursued to recoup costs incurred from unauthorized use of resources or incident response due to a system compromise or malicious activity.
- Criminal penalties could result from violations of federal, state, or local laws. Incidents may be reported to the appropriate authorities for investigation and/or prosecution.

#### **6.0: Classifications of Data**

While TeraGrid partners support the spirit of open research, each provides technology to safeguard the confidentiality of data. Users are responsible for applying these tools effectively to protect intellectual property or confidential data used with or stored in TeraGrid resources.

##### **6.1: Confidential Data**

Users must know if there are confidentiality requirements associated with the type of data they are using. Not all information that is subject to confidentiality is intellectual property. Users are responsible for verifying that the TeraGrid RP site offers the level of protection that is required for the type of data being used.

##### **6.2: Proprietary Data**

Proprietary or private data (which may also be considered intellectual property) may have confidentiality requirements imposed by the owner of the data. Users are responsible for verifying that the TeraGrid RP site offers the level of protection that is required for the type of data being used.

### **6.3: Regulated Data**

State and federal laws as well as organizational policies may apply to the regulation of certain data. Some examples include:

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

It is your responsibility to be aware of the laws and policies that are associated with the data you are managing and to verify that the TeraGrid RP site used can provide the appropriate level of protection.

### **6.4: Sensitive but Unclassified Data, Applications, and Resources**

Some data, applications, and/or TeraGrid RP resources themselves may be considered "Sensitive but Unclassified" or "Export Controlled" by the federal government and may have restrictions and protection requirements. For example, at some RP sites there may be restrictions on the country of origin of users. These restrictions apply to Science Gateway projects as well. It is your responsibility to comply with these restrictions and requirements. For activities subject to these restrictions, a written institutional agreement must be obtained from each RP site before using their resources. Questions regarding export control should be directed to the RP site of interest.

### **6.5: Intellectual Property**

The TeraGrid subscribes to NSF rules associated with intellectual property. As a user, you are required to follow all laws that pertain to any intellectual property that is in your care. For more information, see: <http://www.nsf.gov/od/ogc/intelprop.jsp>

### **7.0: Software Development**

Software that is developed with allocations approved by the NSF, or by proxy via the TeraGrid allocations process, is subject to copyright restrictions according to the NSF General Grant Conditions (GC-1). See the July 2002 revision of GC-1, *Copyrightable Material*, Article 18: [http://www.nsf.gov/awards/managing/general\\_conditions.jsp?org=NSF](http://www.nsf.gov/awards/managing/general_conditions.jsp?org=NSF)

### **8.0: Proper Acquisition and Licensing of Software**

All software used on TeraGrid systems must have been appropriately acquired and properly licensed. Possession or use of illegally copied software is prohibited. Likewise users shall not duplicate copyright-protected software or materials, except as permitted by the owner of 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.

## **9.0: Publication**

All work performed under a TeraGrid grant must be intended for publication in open literature. No proprietary or otherwise restricted publication may be based on work done under a TeraGrid grant.

### **9.1: Acknowledgment of NSF, TeraGrid, and Resources Used**

Acknowledgement of support from the NSF, TeraGrid, and appropriate RP site should appear in the publication of any material (whether copyrighted or not) that is based on or developed wholly or partially with TeraGrid resources.

The following wording can be adapted as necessary. Replace the bracketed information with appropriate content. Visit the [TeraGrid User Info page](#) for links to resource and system information. A copy of each publication should be emailed to [allocations@teragrid.org](mailto:allocations@teragrid.org).

- "This research was supported in part by the National Science Foundation through TeraGrid resources provided by [relevant RP sites] under grant number <TG-xxxx>. [We specifically acknowledge the assistance of <relevant staff members' names>]"

## **10.0: External Requirements in Addition to TeraGrid's**

Individual sites may be subject to state or local laws and/or have organizational policies with additional requirements beyond this policy. It is your responsibility to be aware of and abide by those laws and policies. Please contact the legal affairs department at your home institution for further guidance.

### **10.1: External Requirements for Non-Academic Users**

Non-academic (corporate/industrial, government, etc.) users frequently must follow more stringent usage guidelines than those required by the TeraGrid as a whole or by a particular TeraGrid RP site. It is the user's responsibility to assure the TeraGrid resources used satisfy the requirements of their organization.

## **11.0: TeraGrid Support/Diagnostic Access**

Authorized TeraGrid site personnel may review files for the purposes of aiding an individual or providing diagnostic investigation for TeraGrid systems. User activity may be monitored as allowed under policy and law for the protection of data and resources. Any or all files on TeraGrid systems 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 foreign and domestic. By using TeraGrid systems, users acknowledge and consent to this activity at the discretion of authorized site personnel.

### **11.1: 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.

## **12.0: General Assistance**

For general assistance with understanding this policy or how to fulfill your responsibilities as a user of TeraGrid resources, contact [help@teragrid.org](mailto:help@teragrid.org).

----- Complete and return this page within 30 days -----

## Acceptance Statement

I have read the TeraGrid User Responsibility Form (URF) and acknowledge that I understand my responsibilities as a user of TeraGrid resources. I agree to abide by the stated policies and procedures. I am aware that TeraGrid may occasionally change this document and will inform users when that happens. I acknowledge that I am responsible for reading and understanding all future changes each time I apply for an allocation of resources.

I know that I can find the most current information on the TeraGrid.org web site in HTML and PDF formats:

[http://www.teragrid.org/userinfo/access/user\\_responsibility.html](http://www.teragrid.org/userinfo/access/user_responsibility.html)

[http://www.teragrid.org/userinfo/access/user\\_responsibility.pdf](http://www.teragrid.org/userinfo/access/user_responsibility.pdf)

---

This page must be completed and received by the TeraGrid Allocations Department within 30 days each time you submit an application for resources. The form may be sent via email, fax, or US mail.

If by email, send to: [help@teragrid.org](mailto:help@teragrid.org).

If by fax, send to: 1-217-265-0524

If by US Mail, send to:

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

Name: \_\_\_\_\_

Institution: \_\_\_\_\_

E-Mail: \_\_\_\_\_

Daytime Phone: \_\_\_\_\_

Academic status: \_\_\_\_\_

Date: \_\_\_\_\_