Draft XSEDE Security FAQ

I have sensitive data (e.g., ITAR, HIPAA, dbGaP) used for my research, can XSEDE be used for my work?

XSEDE provides tools and services to researchers that connect to and access compute resources, but does not itself run the resources that are used to store or process scientific data. Resources such as HPCs are run by service providers who participate in the XSEDE federation, for example, by using our identity services for access or allocation services for accounting and provisioning.

Therefore, your research data sets are held by individual service providers and potentially transferred by third parties like Globus Online, and as such the data protection capabilities differ based upon the service provider. By contacting help@xsede.org, we can help put you in touch with representatives at the appropriate parties to answer questions specific to your data security needs.

Where as a PI can I learn how to protect my data and analyze the risks to my intellectual property?

First, you should seek out the expertise at your home institution as they may have applicable security standards and policies. Different institutions have different local laws and interpretations of regulations as well as varying levels of risk tolerance.

However, XSEDE provides some online security training, and the National Science Foundation has funded Trusted CI as a center to help PI’s navigate these issues.

What information does XSEDE collect about me and how do they use it and protect it?

XSEDE maintains a central database which holds information you submit as part of your XSEDE profile on the XSEDE User Portal as well as allocation information to track usage across XSEDE allocated resources managed by various service providers. We also maintain authentication services such as certificate authorities and a Single Sign On hub for central login, with very limited storage capabilities.

More information on the data XSEDE collects and how it is used can be found in the XSEDE privacy policy found on XSEDE’s security page.

Who do I contact in the event of a security issue?

If you suspect a security incident or if your account has been compromised please contact the XSEDE Help Desk immediately via this web form, phone 1-866-907-2383, or send email to help@xsede.org. The help desk uses the XSEDE Ticketing System and will assign your form submission to a ticket. You will receive auto-notification back that lets you know your email has been received, and provides you with a ticket number for reference.

What are my security responsibilities as user, as a PI?

All users are responsible for protecting their XSEDE accounts, using resources for the purposes they are granted access, and following applicable laws and regulations.

PI’s are further responsible for the users on their allocation, making sure the correct people are given access and only those people. The PI must also ensure users on their allocation have accurate XSEDE account details (contact information & institutional affiliation). Further PIs may be held accountable for misbehavior or users they have granted access. PIs must also remove users from their grant when a researcher/student as left the collaboration.

Further PIs may be held accountable for misbehavior or users they have granted access.

All of this is spelled out in greater detail in the Acceptable Use Policy all users sign when their accounts are created.

What security standards and practices does XSEDE follow?

XSEDE participates in security working group’s with national and international partners who provide similar services for open scientific research. Like most of these organizations we align to similar policies and standards and the Security for Collaborating Infrastructures Trust Framework.

Through these collaborations XSEDE has developed a suite of policies, standards and guidelines that can be found on XSEDE’s security page.

How can I better protect my account?

We strongly recommend users make use of Multi Factor Authentication (MFA) services provided by Duo Security. By using a phone app or texting an additional code when you login, it makes it much more difficult for your account to be hijacked.

Not all XSEDE services use MFA, but some such as the Single-Sign-On hub require it. You can activate MFA for your account here.
What is the role of XSEDE versus the service providers for security?

XSEDE provides tools and services to researchers connect to and access compute resources, but does not itself run the resources that are used to store or process scientific data. Resources such as HPCs are run by service providers who participate in the XSEDE federation, for example, by using our identity services for access or allocation services for accounting and provisioning. Consequently, XSEDE’s security program focuses on coordinating organizations for incident response; providing a secure and robust trust framework for authentication services; and protecting the XSEDE Enterprise Services, which are typically systems with the xsede.org domain name but not subdomains like tacc.xsede.org.

How can I get a user x509 certificate?

XSEDE users with an active allocation can get a certificate from the XSEDE MyProxy service for GSI SSH login to XSEDE resources and more.

I am a service provider, how can I get an xsede.org host certificate?

Science gateway operators and XSEDE Enterprise Service administrators can request an xsede.org certificate for their service. This cannot have alternate names for other domains as XSEDE cannot issue non-XSEDE domain certificates with its service.

Service providers who need a certificate with their domain and an xsede.org subdomain can register their subdomain with the InCommon certificate service if their institution is a member. This would allow them to get a certificate within the xsede.org realm and their own institution’s.

Where can I find security training materials?

XSEDE provides security training at the PEARC conference during the new user’s training. Those same materials are available in an online format you can review at any time.

What are the SSH fingerprints for XSEDE allocated resources?

XSEDE Resources SSH Keys are available so anyone can verify the SSH fingerprint the first time they connect to a new resource.

What is the XSO, XSWoG and the XSEDE Trust Group?

- **XSEDE Security Office (XSO):** This is the level 3 security operations manager(s) in XSEDE who sets the work agenda for XSEDE security operations and leads the XSEDE Security Working Group.
- **XSEDE Security Working Group (XSWoG):** This group is responsible for creating security policies and procedures to be approved by the XSEDE Senior Management Team, as well as helping to realize the goals set forth for XSEDE security operations. At a minimum, this group has the XSO, funded members of XSEDE security operations, and a representative from each Level 1 Service Provider (SP). Additional representatives and service providers may join upon approval of the XSO, and this generally includes Level 2 SPs.
- **XSEDE Trust Group:** This is a group largely overlaps with the XSWoG, but also contains other parties with whom XSEDE shares intelligence. They have responsibility for additional calls, keys for encrypted communications, and separate conference call numbers.