XSEDE Level 1 Service Provider security Agreement

Feb 14, 2019

Version 1.2

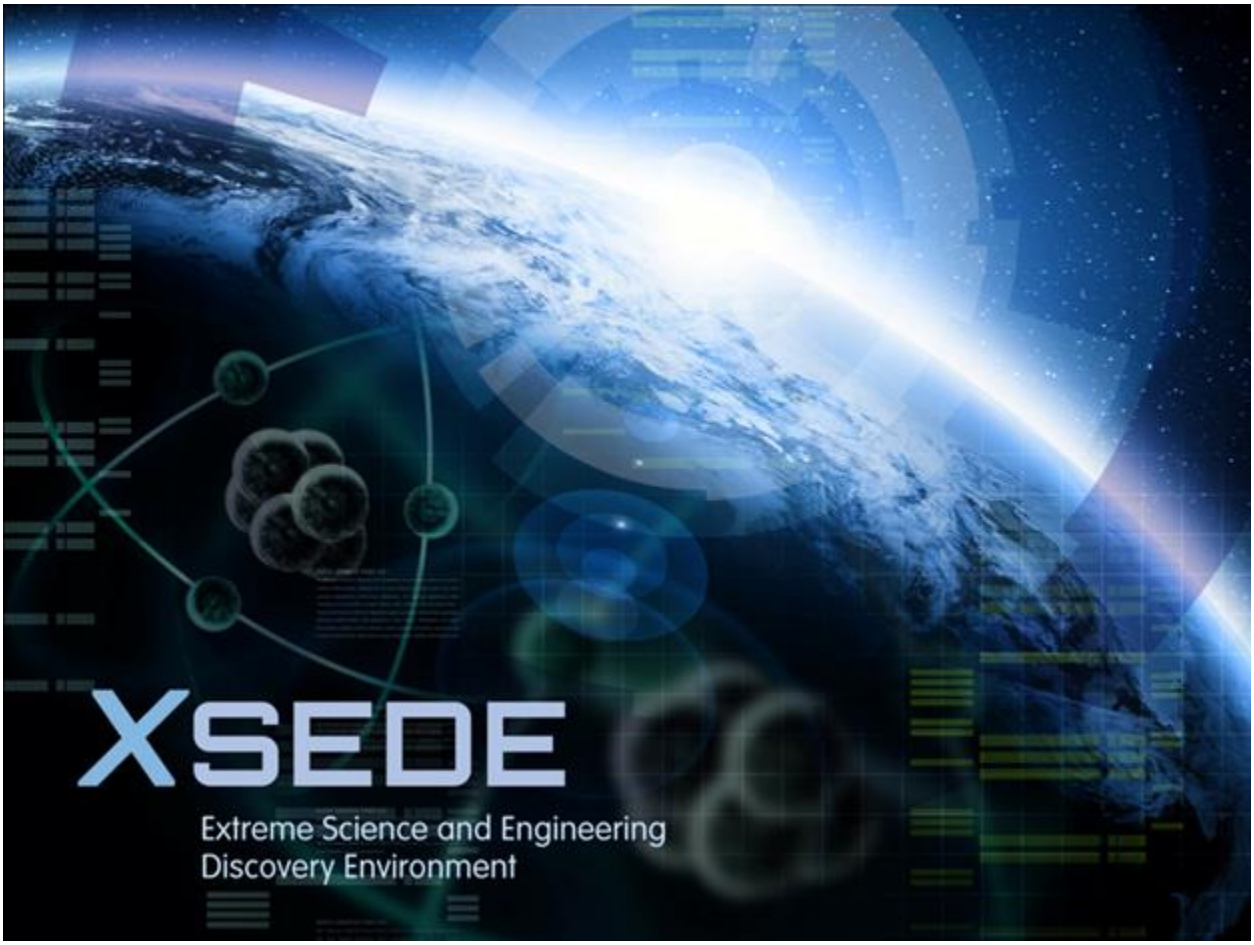

Table of Contents

A. Document History

Relevant Sections	Version	Date	Changes	Author
Entire Document	0.1.5	10/3/2013	Baseline	A. Slagell
Entire Document	1.0	1/1/2015	SP Forum Feedback	A. Slagell
Entire Document	1.1	3/31/16	Updated defn of XSO and IR Team to Trust Group	A.Slagell
Entire Document	1.2	2/14/19	Updated meeting requirements and importance of information sharing restrictions.	J. Marsteller

B. Document Scope

The purpose of this agreement is to define the expectations and responsibilities of the XSEDE Level 1 service providers with respect to security and incident response. This agreement between these service providers and XSEDE lays down the foundation of the relationships necessary to (i) protect XSEDE assets, (ii) respond to threats to those assets, and (iii) maintain the lines of communication necessary for the former two goals.

C. Document Body

C.1. Introduction

The purpose of this agreement is to define the expectations and responsibilities of the XSEDE Level 1 service providers with respect to security and incident response. This agreement between these service providers and XSEDE lays down the foundation of the relationships necessary to (i) protect XSEDE assets, (ii) respond to threats to those assets, and (iii) maintain the lines of communication necessary for the former two goals.

In addition to the Level 1 service providers, there are several important roles for security operations in XSEDE:

- **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 Advisory Board, 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.
- **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.

C.2. Participation

Participation from all Level 1 SPs is vital for a healthy XSWoG and to realize the security goals of XSEDE for its users and participants. As such, XSEDE Level 1 SPs agree to:

- Regularly participate in the regular XSWoG calls
- Participate in the regular XSEDE trust group/incident response calls
- Provide a point of contact for incident response and have their own incident response plan
- Promptly respond to communications about XSEDE security incidents and promptly report XSEDE relevant security compromises at their institution

Specific response times vary depending upon the details of a situation, but responses should come within 8 hours, sites should be able to disable accounts within the same business day, and within 8 hours of realizing a security incident at their site could affect XSEDE they should notify the XSO and XSEDE Trust Group.

C.3. Responsibilities

In addition to simply participating in meetings and responding to important communications, there are several responsibilities with respect to security that each Level 1 SP has. In this section we go through each of these.

C.3.1. Cooperate in Investigations

Beyond just reporting security incidents, the site's incident response point of contact is expected to actively participate in investigations as appropriate. This means sharing information (potentially anonymized) and looking for specific activities on their XSEDE systems related to an incident. It also means that the site must keep appropriate logs for XSEDE relevant systems so that they can cooperate should an XSEDE incident involve their site.

C.3.2. XSEDE CA Tarball

XSEDE Level 1 SPs agree to keep up-to-date with the set of valid XSEDE certificates for both security and compatibility. They should promptly (no more than a week) install new certificates, and report any CA compromises that they are aware of. Sites are of course free to trust additional CAs, such as, a local CA of theirs, but no one else is obligated to do so unless that CA's certificate is in the official tarball.

C.3.3. Vulnerability Identification

As serious vulnerabilities are made known, some of them will impact XSEDE resources. Each Level 1 SP needs to be able to quickly determine if a particular vulnerability could be exploited on an XSEDE relevant system at their site, and if so, they must work with their staff to patch or mitigate the vulnerability in a timely manner and report vulnerability status back to the XSEDE Trust Group.

C.3.4. Protect Sensitive Information

As members of the XSWoG, and even more so of the XSEDE Trust Group, members are privy to much private information (e.g., phone codes, PGP keys, wiki accounts, etc.). As such, these members are expected to protect these credentials and not share them with anyone else without approval from the XSO.

In addition to these many credentials, members of these groups may be privy to sensitive information regarding security incidents and security defenses at other institutions. They must respect the privacy of these other institutions and only share incident relevant information within their organization as needed to resolve the incident.

C.3.5. Security & Privacy Policy Awareness

Each Level 1 SP agrees to make any local security and privacy policies available and easy to find for XSEDE users who may be running jobs on their systems.

C.3.6. XSEDE Security Baseline Document

There are security baselines for running XSEDE central services that SPs providing such services are required to follow. These baselines are approved by the XSWoG, on which each Level 1 SP is given representation.

Sites may need to deviate from the baseline requirements; in these cases an exception should be requested. Exceptions must be scoped as small as possible and be approved either by the XSO or the XSEDE Project Office.