Stanford School of Earth Sciences.

Security Policy for Confidential Data Acquired from a Third Party for Research Purposes

The purpose of this policy is to insure security of research data acquired from a third party with the understanding that the data themselves will be kept confidential. This is particularly critical if the data were acquired through a non-disclosure agreement, signed either by a faculty member or by the Industrial Contracts Office on behalf of the University. The faculty member(s) that is (are) responsible for the research group accepting the data is (are) also responsible for policy implementation. This policy guides how Stanford will handle the data internally and prevent disclosure to third parties. It does not govern data transfers and communications between Stanford and the data owner.

This policy is intended to provide guidelines and to be in compliance with University requirements for data classification, access, transmittal, and storage of "confidential data", as described at:
http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html .
Individual non-disclosure agreements may modify terms of these policies in a manner that is acceptable to both the data owner and Stanford.

This policy applies to all confidential research data that are stored electronically, whether it be in numeric, text, graphical, or other formats. This policy also applies to all derivatives, transformations, and analyses of the original data that may reveal the confidential information contained in the data. Derivative products such as presentations, figures, and papers that do not reveal the confidential information are not covered by this policy, but their distribution may be subject to restrictions or approval requirements in the non-disclosure agreement. Once a publication or presentation based on confidential data has been approved for distribution by the data owner, it is no longer subject to this policy.

Access to the data and their derivatives will be limited to specific SUNet IDs of the individuals authorized by the Principal Investigator or his/her designee. Working electronic copies of data may only be stored on an approved server that is physically secured, professionally managed, and includes access controls to limit access rights by SUNet ID. Data analysis is to be performed by accessing the data directly from the server as well as storing all intermediate and derivative products in the restricted area on the server. Temporary copies may be made on local disks of compute cluster nodes provided deletion is automatic upon completion of the analysis run. Backups must also be stored securely; any "cloud" (third party network) backup must be fully encrypted.

No data copies or derivatives shall be made or stored on any local computing device or local storage device, including external hard drives, flash memory drives, or optical media, unless those devices are fully encrypted or maintained in locked and secured facilities.

Feb. 2013

Only Stanford-owned and maintained computing systems that have been secured by School IT staff may be used to access and analyze the data. Workstations used for analysis may not enable public file sharing or install peer-to-peer sharing software, since common configurations may expose the confidential data accessed by the workstation to the Internet.

Three server storage options are approved by this policy, and the School's Information Technology Manager may approve others that shall be listed in an Appendix:

1. Restricted file shares created on the School of Earth Sciences file server cluster. This is an appropriate storage location for general-purpose analysis, including analysis from workstations or the CEES computers. This server has integrated secure disk and tape backup facilities.
2. Restricted directories created by the system manager on the file storage systems of the CEES computing clusters. This is an appropriate storage location for analysis of large amounts of data on the actual cluster nodes. This server has no designated long-term storage, with backup options limited to mirroring - consult the School IT Manager for further backup options.
3. Files shares provided on storage servers maintained by the campus Information Technology Services group. Tuhis is appropriate for analysis on workstations, but is not accessible to CEES. These servers have integrated basic disk backup with short retention. See: http://itservices.stanford.edu/service/storage/chart

Everyone with access to the data must be made aware of the “Security Policy” described in this document, and trained on how to fulfill its requirements. In particular, everyone with access to the data must be trained not to write output data files onto local media, including but not limited to local or external disk drives, CD/DVD, and flash memory storage devices, except when those devices are fully encrypted. Users should immediately report any event that could potentially lead to data loss or theft, such as suspected hacker compromise of a computer used for data analysis, to the School's Information Technology Manager or Network Administrator.

Appendix

Last revision October 2, 2014

Additional file servers approved for storage of confidential research data in the School of Earth Sciences:

Server Name and Description	Location	Manager	Access controls	Backups
Sherlock	Stanford Research Computing Center	Ruth Marinshaw ruthm@stanford.edu	Kerberos login required, soon dual authentication. Standard Linux permissions limit access to any directory to SUNet IDs in specified group.	Copies to other servers managed by SRCC
Stanford Exploration Project compute cluster parallel file system.	Mitchell 467 - locked computer server room.	Bob Clapp, bob@sep.stanford.edu SEP, Geophysics Department.	File servers connected to separate internal network for access by compute nodes only. Not visible to internet. Standard Linux permissions limit access to any directory to SUNet IDs in specified group.	Copies to additional disks stored in locked computer room.