

SDSC Services Standards & User Responsibilities

SDSC Regular Business Hours

- We have defined “Regular Business Hours” as **Monday through Friday from 0800 to 1700, Pacific Time**. Campus holidays are not included in regular business hours.

Advanced Notifications of Scheduled Downtime

- For non-critical maintenance, SDSC will provide a minimum 14 calendar days advance notification via email to opsnotice@sdsc.edu. Some notification messages may include maintenance windows where downtime is not required.
- Customer will communicate the scheduled maintenance with their user community as appropriate.
- Customer is responsible for subscribing to the OpsNotice mailing list at:
 - <https://lists.sdsc.edu/mailman/listinfo/opsnotice>

Communication Regarding Unscheduled Downtime

- If critical security patches are released that will require downtime and pose an immediate security threat, SDSC will provide as much advance notice as is feasible, however a non-standard emergency downtime may be taken to maintain system integrity and security.
- Upon resolution of an emergency downtime due to security or other unplanned outage, SDSC will attempt to notify affected groups within 4 business hours.
- Within one business day, SDSC will provide a written post-incident summary (high-level, 1 page, 1-3 paragraphs) to opsnotice@sdsc.edu including:
 - What went wrong
 - Solution
 - Recommended preventive measures and other lessons learned

Technical Support Procedures

- Low Priority Issues
 - *Examples: User configuration problems, issues affecting single-users, issues with most research systems during off hours.*
 - Submit via email to support@sdsc.edu.
 - Automated receipt acknowledged within 1 hour.
 - SDSC technical team follow-up by close of following business day.
- High Priority Issues
 - *Examples: Issues affecting entire user communities, issues with production resources on which there are multiple dependencies from other services.*
 - Submit via phone call to SDSC Operations: (858) 534-5090.
 - SDSC Operations will take pertinent information, including incident details and response phone number, create a support ticket, provide the tracking number to the customer, and telephone on-call member of SDSC technical team supporting the project.
 - SDSC technical team follow-up by phone as soon as possible – response goal: 4 hours.
- Critical Priority Issues
 - *Examples: Service downtime affecting entire user communities that require immediate access to the service, Downtime of resources on which there are multiple dependencies from other services.*

- Submit via phone call to SDSC Operations: (858) 534-5090.
- SDSC Operations will take pertinent information, including incident details and response phone number, create a support ticket, provide the tracking number to the customer, and telephone on-call member of SDSC technical team supporting the project.
- SDSC technical team follow-up by phone as soon as possible – response goal: 1 hour.

User Responsibilities

Users of SDSC's services shall insure that the following conditions are met:

- **Appropriate Data:** Customer shall insure that all data stored at SDSC is consistent with the stated Customer's data description in the service agreement. Data and programs of a personal or pornographic nature are inappropriate for storage at SDSC. PII (Personally Identifiable Information) and information protected by HIPAA (Health Insurance Portability & Accountability Act) privacy rules are inappropriate for storage within the SDSC Storage Services facility without proper encryption and coordination with SDSC Security.
- **Use and Distribution of Data Stored at SDSC.** It is Customer's responsibility to ensure that Customer has all required rights (copyrights, licenses, etc.) to possess copies of data to be stored at and further distributed from SDSC. Storage and/or distribution of data at SDSC to which Customer does not have full rights will be considered a violation of this agreement and grounds for immediate termination.
- **Security:** Customers are responsible for the security of their systems, services, and data. Systems and services hosted at SDSC shall be maintained by the customer unless otherwise coordinated and described in the customer's service agreement. Users are required to protect their password(s). Passwords must **never** be shared. A customer who believes a password has been compromised should change that password immediately and inform SDSC as soon as possible.
- **Backups of Critical Customer Data:** Customers are responsible for backing up critical data. File systems and archival storage systems are very reliable; however, data can be lost or damaged due to media failures, hardware failures and human mistakes. For these reasons, SDSC strongly encourages Customers to maintain multiple copies of critical data: at least one copy at the customer's site (or other offsite, non-SDSC site) and one or two copies at SDSC. "Dual" copies referred to in storage service agreements are for two copies at SDSC and do not imply offsite storage of any kind.