National Research Platform Acceptable Use Policy

Draft 0.1

When you receive access to any of NRP services, and every 12 months thereafter, you will be asked to accept and re-acknowledge your responsibilities regarding use of systems and services of NRP. These provisions are in addition to any you are subject to at your institution.

NRP has legal obligations to protect shared services and resources. You share this responsibility by observing and upholding the rules of acceptable use that are outlined in this document.

Your on-line assent to this Acceptable Use Policy (AUP) is your acknowledgment that you have read, understand and accept your responsibilities when using NRP services. If you have questions, please contact the NRP via the NRP Matrix chat or by submitting a ticket to the NRP Helpdesk at support@nationalresearchplatform.org.

Violations of this AUP may result in loss of access to NRP resources. Activities in violation of any laws will be reported to the proper authorities for investigation and prosecution.

By using NRP-managed services and resources associated with an NRP allocation (hereafter, "NRP services and allocated resources"), you agree to comply with the following conditions of use:

1. NRP does not provide services or resources that satisfy the security requirements for handling or processing HIPAA, PII, CUI, FERPA, or any other data protected by statute or data-use agreement. You agree to not introduce these types of data to NRP resources.
2. You understand that NRP does not guarantee that resources and services will be available, that they will suit every purpose, nor that data will never be lost or corrupted.
3. You agree to protect all accounts (i.e., IDs, account names, usernames) and credentials (e.g., passwords, private keys, tokens and [DUO or other] authenticator codes) that you use to authenticate to NRP resources.
4. You agree to not use NRP services nor allocated resources for any of the following:
   - financial gain
   - any unlawful purpose
   - attempt to breach or circumvent any NRP administrative controls or security controls
   - in violation of any agreement or terms-and-conditions of software or data introduced to these NRP resources.

   You agree to comply with all applicable laws and relevant regulations, such as export control laws and HIPAA.
5. You agree to immediately report any known or suspected security breach or misuse of your access to security [at] sdsc.edu You understand that you are responsible for backing up your data. Use of NRP services and allocated resources is at your own risk.
6. Logged information, including information provided by you for registration purposes, is used for administrative, operational, accounting, monitoring and security purposes. This information may be disclosed, via secured mechanisms, only for the same purposes and only as necessary to other organizations cooperating with NRP. You authorize the collection and sharing of this data for the purposes described above. Further, you understand that to preserve log integrity for security reasons, the collected data cannot be deleted until it is naturally aged-out by a data-retention policy.
7. In manuscripts submitted for publication and any other citable works, you agree to acknowledge NRP services and resource(s) contributing to research results with the following language
   - This work used resources available through the National Research Platform (NRP) at the University of California, San Diego. NRP has been developed, and is supported in part, by funding from National Science Foundation, from awards 1730158, 1540112, 1541349, 1826967, 2112167, 2100237, and 2120019, as well as additional funding from community partners.