Douglas Neuroinformatics Platform Terms of Service v1.1

The Douglas Neuroinformatics Platform (DNP) is a computing system exclusively for use as a tool to store, process and aggregate data for the Douglas Hospital Research Centre (DRC).

Definitions

Account Holder: an individual who has a Douglas Neuroinformatics Platform (DNP) account.

1. Access to Resources
    1.1. You will never access or attempt to access any DNP resources (or any other user's data on the DNP resources) other than those resources or data to which you have been granted access by a DNP administrator.
    1.2. You will always abide by any policies, protocols, or requirements that are in effect at institutions with which you are affiliated, such as an Acceptable Use Policy. In a situation in which a conflict exists between the DNP Terms of Service and the policies at institution(s) with which you are affiliated, you must notify the DNP staff and comply with any requirements identified by the DNP staff.
    1.3. You will not allow any other individual to use your account to access DNP resources. If others require access as part of your research, these individuals must apply for their own account.
    1.4. Any DNP account credentials and information used for authentication are confidential and you are responsible for keeping them secure. Failure to do so may result in account suspension, see 4 below.
2. Conduct Requirements
    2.1. You are responsible for the activities associated with your account and for the use of resources assigned to you.
    2.2. You are responsible for understanding and meeting any privacy, confidentiality and acceptable use policies, requirements, laws or regulations that apply to your research and data. This includes, for instance, any provincial privacy laws or ethics board requirements affecting any data (e.g. clinical or personal health information) that you store on DNP systems.
    2.3. In the event, your account is compromised, or suspicious activity is detected related to resources assigned to you, you agree to work with DNP staff and any institution with which you are affiliated to resolve the issue.

2.4. At no time will you use DNP resources for any activity that contravenes any applicable laws or regulations. You are responsible for identifying all applicable laws and regulations that may apply.

2.5. You agree that should you ever be investigated or found liable for any contravention of Canadian law, or any other applicable laws, the DNP is in no way responsible or liable for such contraventions or for any penalties associated with it. If anyone attempts to make the DNP liable for anything related to your research or your use of DNP resources, you agree to work with DNP staff to address the issue.

2.6. You must immediately notify the DNP if you become aware of any unauthorized access or use of DNP resources or data or of any event that might affect DNP information security or privacy.

2.7. You will complete an annual account renewal process to retain access to resources assigned to you.

2.8. The DNP reserves the right to define abuse of resources and take appropriate action where and if necessary. For example, it has the right to monitor use of its systems, deactivate an account, or block access to DNP resources.

2.9. On services where you can interact with other users or staff of DNP, you shall conduct yourself with all due civility.

3. Use of Resources

3.1. You will not use the DNP resources in any situation in which failure or fault of the use of the resources could lead to death or serious injury of any person or animal, or serious physical or environmental damage.

3.2. You will not introduce software into the DNP environment that may damage, interfere with, or capture any system, program, or data outside of your own assigned resources. The DNP reserves the right to identify, quarantine or delete any such software, as well as any related data.

3.3. You will not attempt to probe, scan, penetrate or test any DNP services or systems for vulnerability nor to probe, scan, penetrate or test any external services or systems.

3.4. You will not try to access or intercept data not intended for yourself or for the resources that are assigned to you.

3.5. You will not send or assist with unsolicited bulk communications.

3.6. You will not use applications without valid and appropriate licensing.

3.7. You will not use software services that would override DNP authentication or policy enforcement.

3.8. You will not use software or services that provide unprotected access to shared DNP resources.

3.9. You will not knowingly use DNP resources in a manner that impedes or denies the ability of others to use the resources to which they have been granted access.

3.10. You are expected to use DNP resources efficiently.

4. Suspension of access and Termination

4.1. Failure to abide by these Terms of Service may result in temporary or permanent revocation of access privileges as well as legal action against you or your institution.
4.2. If access is revoked or expired, the DNP will archive or retain your data for a one-year period. Temporary data (scratch) will not be preserved and may be deleted at any time. After a year, if no action has been taken to reactivate the account, the DNP reserves the right to permanently delete all of your data.

5. Provision of Service
5.1. The DNP reserves the right to request documentation that demonstrates that proper authorization is in place for the use of DNP resources.
5.2. The DNP reserves the right to audit and monitor the usage of, performance, and security posture of its systems to manage service stability, integrity, accessibility, and confidentiality.
5.3. To maintain overall system performance, the DNP reserves the right to manage system load. This may include deactivating logins, killing processes, or deleting jobs without notice to protect operational stability.

Changes

1.0 -> 1.1
Drop DNP WiFi Services