Cluster Computing Resource User Policy

MRI Center, NYSPI

MRI Center Staff (Adapted from FRSecure AUP V1.0 8/2021 Draft)

6/2022

Purpose

The purpose of the Cluster Computing Resource User Policy is to establish acceptable practices regarding the use of NYSPI MRI Center information resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Audience

The Cluster Computing Resource User Policy applies to any individual, entity, or process that interacts with any NYSPI MRI Center information resource, inclusive of NYSPI XNAT, on premise and cloud processing environments, and share storage solutions.

Acceptable Use Policy

* Personnel are responsible for complying with NYSPI MRI Center policies when using NYSPI MRI center resources.
* Personnel must promptly report harmful events or policy violations involving NYSPI MRI Center assets or information to NYSPI MRI Center staff or psyIT. Events include, but are not limited to, the following:
  + Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to NYSPI MRI Center information resources.
  + Data incident: any potential loss, theft, or compromise of NYSPI MRI Center information.
  + Unauthorized access incident: any potential unauthorized access to a NYSPI MRI Center information resource.
  + Facility security incident: any damage or potentially unauthorized access to a NYSPI MRI Center managed lab space.
  + Policy violation: any potential violation to this or other NYSPI MRI Center policies, standards, or procedures.
* Personnel should not engage in any operation known or reasonably suspected to significantly degrade the performance of the processing or storage systems utilized by the NYSPI MRI Center information resources without prior approval from MRI Center staff for each case. Such operations include, but are not limited to:
  + DICOM file processing and handling, including moves and copies, involving multivolume series (file count > 600) on MRIdoctor
  + Any operation on XNAT which changes session metadata or causes archive data to be moved within the archive that has not been approved prior
  + Any transfer of imaging data to MRIdoctor not consistent with MRI Core’s service offerings or mission
* Personnel should not purposely engage in activity that may:
  + harass, threaten, impersonate, or abuse others;
  + degrade the performance of NYSPI MRI Center information resources;
  + deprive authorized NYSPI MRI Center personnel access to a NYSPI MRI Center information resource;
  + obtain additional resources beyond those allocated;
  + utilize information resources for purposes outside of or contrary to the mission of the NYSPI MRI Center;
  + or circumvent NYSPI MRI Center computer security measures.
* Personnel should not download, install, or run programs or utilities on any NYSPI MRI Center resource that have not been approved. The NYSPI MRI Center maintains all code, operating systems, and installations required for users to fulfil the intended purpose in utilizing the provided information resources.
* Use of encryption should be managed in a manner consistent with the relevant NYS (ITS and OMH), CUMC, and NYSPI policies.
* Personnel are expected to cooperate with inquiries conducted by NYSPI MRI Center staff pursuant to the goal of maintaining the confidentiality, integrity, and availability of information resources.
* Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using NYSPI MRI Center information resources.
* Personnel should not intentionally access, create, store, or transmit material which the NYSPI MRI Center may deem to be irrelevant to the mission of the NYSPI, including but not limited to content considered offensive, indecent, or obscene.
* Personnel should never access, create, store, or transmit PII or PHI using NYSPI MRI Center information resources in any context outside of the established policies of NYSOMH, CUMC, NYSPI and the NYSPI MRI Center. There should never be, under any circumstances, PII on XNAT or MRIdoctor aside from incidental indirect identifiers created during imaging procedures e.g., dates and high resolution facial images.
* Personnel granted access to resources should never share their passwords or credentials even with other staff.
* Research groups granted access to XNAT and the MRIdoctor are fully responsible for their actions which may impact the confidentiality, integrity, or availability of their data and the data belonging to other groups which share the same resources.
* Any information resource that connects to MRI Center information resources must connect using psyIT-approved methods such as the NYSPI VPN or local network and be configured in a manner consistent with relevant NYS, CUMC, and NYSPI policy.
* Information created, sent, received, stored, or processed on MRI Center information resources are not private and may be accessed at any time by MRI Center staff or psyIT in the course of systems operations.
* Certain users may be granted extended privileges that extend beyond those granted to regular personnel. Such users should not use any extended privileges to access any data or processes to which they have not been granted explicit approval to access.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties. Future inclusion in NYSPI MRI Center programs and offerings may be restricted for research groups associated with staff misconduct.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.