NYSPI Authentication Bulletin

To address state and local compliance needs and to ensure the privacy and security of NYSPI data and systems, user access must be carefully managed. Details are including in the NYSPI System Management Procedures found at http://support.nyspi.org. This further references the NYS Account Management and Access Control Standard (http://on.ny.gov/2b3D288), which provides guidance on creating and managing access to data, and the NYS Authentication Token Standard (http://on.ny.gov/2bq4myp) which provides password requirements.

To this end, any NYSPI-hosted system or system serving or storing NYSPI-data must comply with these standards. Specifically, passwords for NYSPI systems must minimally meet the following criteria.

- Passwords must expire at least every 180 days but not sooner than 2 days.
- Systems must prevent "brute-force" attempts by locking the account after 5 incorrect attempts. If support staff are available for the general hours of operation, accounts should remain locked until reset by an administrator after sufficiently verifying the user's identity.
- Passwords must be complex, as defined in NYS standard and not be reusable for 24 unique changes.
- Standard user passwords must be at least 10 characters long. Administrative and/or privileged account passwords must be at least 16 characters long, unless additional dual-factor authentication is required. Use of passphrases is to be encouraged.

While NYSPI encourages used of the NYSPI AD for consolidated authentication, limiting the number of passwords staff need to remember, users are encouraged to use a personal password vault, as this will help encourage the use of strong passwords and limit forgotten passwords. Password vaults must:

- Use strong, federally-recognized encryption for the storage of the password.
- Master keys must be stored locally, not in a cloud solution
- The password vault should be stored locally. Cloud synchronization of an already encrypted vault is OK, but encryption should occur local and cloud should not be the only storage location.

Respected password vault solutions include Dashlane and KeePass.

Tips for setting a strong password can be found at http://bit.ly/2byHLR3

Questions or requests for exceptions should be sent via a service desk ticket or by e-mail to PsyIT-Admin@nyspi.columbia.edu.