NYSPI Systems Management Procedure

Summary

The NYSPI computing environment is designed to support the diverse and ever-changing needs of our world-class research activities. Consistent standards for the management and oversight of all NYSPI technology environments and platforms supports protection of subjects, efficient and agile operations and overall organizational integrity.

NYSPI shall comply with all NYS security Policies and Standards, principally found at https://www.its.ny.gov/tables/technologypolicyindex. Additional processes or actions may be required by regulation, protocols, contracts or other obligations. When requirements conflict, the most restrictive controls shall be applied.

Scope

This procedure shall apply to all technology developed or operated for NYSPI or within the NYSPI network, regardless of the operators or custodians of the solution or funding source of the operators or systems.

Procedure Statement

1. System Development / Initialization
   1.1. Systems should be developed to support documented and approved business needs only. NYSPI IT (psyIT) will develop and host a secure, searchable repository for system documentation.
   1.2. Each system must have a documented information owner and custodian submitted to NYSPI IT (psyIT) prior to development and/or implementation
   1.3. System compliance requirements, including record auditing and availability requirements, must be documented. These records should be kept as part of overall system requirements and document as described in the NYS Secure System Development Lifecycle Standard (http://on.ny.gov/2b6slAq).
   1.4. psyIT will collaborate with key NYSPI administrative and research teams to develop and publish a list of preferred technologies and their recommended use. These technologies should be used whenever possible. Use of competing technologies must be documented and approved by psyIT.

1.5. psyIT will publish and maintain a list of shared solutions, which will be systems managed by one group for use by others in NYSPI. These solutions may be hosted by psyIT directly or through partnership with advanced technology groups through NYSPI or NYS. Shared solutions should be used whenever available and able to address the documented business requirements. Use of shared services can be requested through the standard NYS service request ticket processes (NYSITSM).
1.6. psyIT may develop additional procedures and standards for the use and operations of specific shared services.
1.7. Any new system leveraging open source or commercial solutions must be built using a version of that solution which is at least 1 level above the minimum supported version, where multiple versions are supported.
1.8. The NYS Secure Configuration Standard (http://on.ny.gov/2bnwtx7) provides guidance for checking the configuration of many types of systems. psyIT recommends using community-validated configuration benchmarks from CIS (http://bit.ly/2bNl2zV) and will make benchmark bundles available for use on NYSPI networks and systems available from the psyIT intranet website. The configuration of a representative sample of all systems should be reviewed at least annual and after any major modifications.
1.9. Systems must be configured to limit running services to those needed for the function and management of the system.

2. System Maintenance
2.1. To maintain the highest possible level of security and operational stability, available system updates must be applied in accordance with the NYS Patch Management Standard (http://on.ny.gov/2bAoqLX)
2.2. All operating systems must be patched at least monthly
2.3. All platform / middleware software must be patched based on the criticality of the system or data, respecting the risk the solution may have on the shared environments.
2.4. Any system changes, including system patching, shall be completed in accordance with the NYSPI Change Management Procedures.

3. Logging and auditing
3.1. All security events must be logged in accordance with the NYS Security Logging Standard and NYS records retention requirements defined by the NYS Archives (http://www.archives.nysed.gov/records/retention_mi-1_electronic-data)
3.2. Logs for all systems accessible from the Internet or accessed by systems which are accessible from the Internet must be logged to an external system and integrated into the NYSPI-wide enterprise log monitoring service. Use of NYSPI security logging service is required unless otherwise approved by the NYSPI Chief Information Security Officer as an exception described below.
3.3. Applications must implement the record-level auditing defined by applicable compliance requirements and must be secured commensurate with the data contained in those audit records.

4. Account and Access Management

4.1. All requests for access to systems must be documented and approved by the information or system owner.
4.2. In accordance with NYS record retention standards, records of the assignment and approval of system access must be maintained for until the access is revoked or system is retired, unless otherwise mandated.
4.3. All accounts must support all NYS Account Management & Access Control and Authentication Token (a.k.a password) standards, including password strength, change and encryption requirements.
4.4. Where possible, internal NYSPI systems shall use the NYSPI Active Directory for authentication.
4.5. Where direct integration with NYSPI Active Directory services is not possible, a process must be developed to ensure account changes in Active Directory are communicated and reflected appropriately in the active account system.
4.6. Processes must exist to review access to systems at least annually and individuals with access not required for their current duties shall have the access revoked. Systems hosting PHI or PII should be reviewed quarterly where feasible or semiannually, where more frequent review is not feasible. Reviews and results should be documented with system documentation.

Exceptions

Requests for exceptions to these procedures should be directed to the contacts listed below and will be acknowledged within 2 business days or will be automatically approved.

Contact

Questions or requests for exceptions shall be directed to both the director of psyIT and the OMH Chief Information Security Officer. E-mails may be sent to the current individuals directly or to psyIT-Admin@nyspi.columbia.edu .

Review Schedule and Version History

Date	Description of Change
7/29/16	Initial draft
8/1/16	Minor corrections
8/17/16	Final Draft for publication
10/26/16	Removed watermark
12/15/16	Updated configuration benchmark language in System Development / Initialization
9/10/18	Added requirement for account management communications for non-AD account systems (4.5) General review and minor revisions.