NYSPI Endpoint Configuration Bulletin

NYSPI is required to follow NYS technology policies and standards, including the NYS Information Security Policy P03-002 (https://on.ny.gov/2O2SceQ).

As the path to most data is the endpoint – whether a PC, Mac or mobile device – secure configuration of these devices contributes highly to NYSPI security.

The NYS Secure Configuration Standard (http://on.ny.gov/2bnwtx7) provides guidance for checking the configuration of many types of systems, including endpoints. 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 NYSPI psyIT intranet website.

In accordance with NYS and CUIMC policies, all computers connecting to the NYSPI internal network must be full-disk encrypted, routinely patched, configured to limit running services to those needed for the function and management of the system and authenticated with an individual network log in. Systems should be configured to log security events, such as successful and failed logins.

Specific configuration questions should be sent to the psyIT service desk at psyit@nyspi.columbia.edu.