
TITLE: **GENERAL INFORMATION SECURITY POLICY**

POLICY:

Good password, software, network (including Internet) and other security practices are followed for electronic systems, and security awareness training is provided to the workforce members to exercise appropriate precautions against potentially risky behavior.

PURPOSE:

Follow reasonable information security practices, and instruct all workforce members on such practices.

APPICABILITY:

Hospital staff, employees, owners, custodians, and users of information systems

PROCEDURE:

1. **Sensitive Data in Electronic Form**
   Information systems are required to be protected by authentication systems that employ user identifiers (User IDs) and secret passwords unique to each user. Password management procedure includes:

   A. Not sharing passwords and not using other people's passwords to gain system access.
   B. Requiring and forcing regular password changes at a maximum every 180 days. Initial password should be changed immediately.
   C. Preventing frequent reuse of passwords. (Recommend that passwords may only be reused every fourth time.)
   D. Permitting workforce members to select and change their own passwords.
   E. Requiring passwords that meet the following criteria:
      a. Do not use dictionary words or commonly known proper nouns.
      b. Use passwords that are at least eight characters long.
      c. Include small letters, capital letters and numbers.
   F. Requiring passwords to be hidden when entering into information systems.

G. Requiring passwords to be given to workforce members in a reasonably secure manner.
H. Forcing changing of default vendor passwords immediately following installation of hardware and software.
I. Training workforce members on good password practices.

2. Information operating systems and applications should be reasonably configured to guard against malicious software that may pose a risk to information. Malicious software includes bots, viruses, worms, spy-ware, etc.

   Responsibilities of workforce members include:
   A. Refraining from bypassing or disabling protection mechanisms unless authorized to do so.
   B. Reporting suspected or confirmed malicious software.
   C. Exercising caution when accessing web pages from unknown sources.
   D. Delete emails with attachments from unknown sources without opening the attachment.

3. Responsibility of owners and custodians of workstations, servers, and applications include:
   A. Installing and ensuring regular updates of anti-virus (and other protective) software.
   B. Implementing regular security patch procedures for all underlying software including operating system, databases, web and other servers and services, etc.
   C. Configuring systems to guard against accidental or opportunistic misuse of the system. This includes shutting down unnecessary services, ensuring strong passwords for all accounts in all underlying software, and configuring protections of files and databases.
   D. Implementing anti-spam and anti-virus software for email and other mass communication systems.
   E. Maintaining ability to recognize a malicious attack and to recover from such an attack with adequate backup and disaster recovery strategies.
   F. Using Center-Wide Identifier (CWID) to create user accounts. (See *Center-wide Identifier Creation Procedure*.)
   G. Following *Access Request Procedure* to fulfill, track, authorize and document account and access provisioning and changes.
   H. Managing audit logs of platforms (servers, database, web servers, and similar platform environments) and applications using *Platform Audit Log Processing Procedure* and *Audit Log Processing Procedure*, as appropriate.
   I. Participating in risk analysis and documenting security measures taken to meet requirements. See *Risk Analysis Procedure* and *Application Security Documents List*.

4. Workforce members are required to logoff from applications after completing their access at any location that may potentially have multiple users. Owners and custodians should implement procedures in information systems to terminate established sessions after no more than 30 minutes of inactivity through an automatic logoff mechanism or an equivalent alternative mechanism. An exception to this requirement is permitted where the immediate area surrounding a system is physically secured.

5. Workforce members will receive security information, awareness reminders, training, and updates via:

    A. Information system sign-on messages (see ***Information security: audit and evaluation policy*** (#I225))
    B. Pop-up messages, and dialog boxes, as appropriate within applications
    C. Screen savers
    D. Management bulletins through email and mail, as well as communication with staff in seminars and other venues
    E. Annual Training

6. The confidentiality of information at rest and during transit is protected by encryption when it is determined to be necessary, reasonable and appropriate through the risk analysis process. (see ***Information Access Management and Control policy*** (#I215)) Specifically, all desktops, workstations, laptops, tablets, smartphones and other mobile devices must be encrypted.

7. Unless specifically excluded with documentation, all communication of sensitive data over the Internet outside the networks controlled by NYP and its affiliates are encrypted.

8. Unless specifically excluded with documentation, all communication of sensitive data over the wireless network controlled by NYP and its affiliates are encrypted.

9. The integrity of information at rest and during transit is protected by implementing integrity controls such as message hashing, encryption, and reliable transport protocols when it is determined to be necessary, reasonable and appropriate through risk analysis process.

10. The decision to encrypt or establish other integrity controls should be based on the following:
        A. sensitivity of the information
        B. risks to the information

C. expected impact to functionality and workflow if the information is encrypted or has additional integrity controls
D. alternate methods to protect the confidentiality, integrity and availability of the information
E. cost of the additional measures

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Access Request Procedure (IT-CS-002)
Application Security Documents List (IT-SEC-001-F2)
Audit Log Processing Procedure (IT-SEC-004)
Center-wide Identifier Creation Procedure (IT-SEC-006)
Platform Audit Log Processing Procedure (IT-SEC-005)
Risk Analysis Procedure (IT-SEC-001)
Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D), 164.312(a)(2)(iii)

REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Revised: March 2013; **March 2015**