

**MICHIGAN STATE UNIVERSITY
HEALTH INFORMATION TECHNOLOGY
POLICIES/PROCEDURES**

SUBJECT: Password Management **No: IS 8**

**SCOPE: All MSU Medical Areas (HealthTeam, Olin, CHM, COM, CON) Faculty,
Staff and Contract Supported Users** **Page: 1 of 2**

AUTHOR: JJ Strieff, Linda Losik

APPROVAL: Practice Executive Committee

EFFECTIVE DATE: 1/15/2005 REVIEW DATE: 1/15/2007, 12/13/2008 REVISED

DATE: 12/XX/2009

POLICY STATEMENT

The MSU Health Information Technology (HIT) will ensure that a stringent Password policy is maintained for all users. Passwords are an important aspect of computer security as they form the front line of protection for user accounts. A poorly chosen password may result in the compromise of MSU HIT's network. As such, all MSU Medical areas (CHM, COM, CON, Olin and HealthTeam) employees including contractors and vendors, with access to hc.msu.edu systems are responsible for utilizing the guidelines as outlined below to select and secure their passwords.

User accounts that have system-level privileges granted through group memberships or programs such as Centricity or IDX are recommended to have a unique password from all other accounts held by that user.

Passwords must not be inserted into email messages or other forms of electronic communication.

Do not give the password to anyone. If someone demands the password, immediately contact the Security Officers.

If an account or password is suspected to have been compromised, report the incident to the Security Officers and change all passwords associated with the account holder.

PROCEDURE

**All Users: Password
Creation**

- Account holder must create a strong password using the following criteria:
- Must be at least 8 characters long
- Must contain at least one upper case and/or one lower case letter
- Must contain at least one number

- Inclusion of one or more special characters (e.g., @, #, \$) are recommended but not required
- The password cannot contain the user name
- Passwords will be set to expire after 365 days, at which time the user must select a new password.
- Four historical passwords will be stored on the server; when a new password is created, none of the most recently stored passwords can be reused.
- Passwords must not be accessible to, shared with or used by anyone other than the account holder.

Account Lockout: All Users

- Locked out user must call the main HIT line at 355-6531 to request an account to be unlocked.
- Must have Z-PID or A-PID to identify over the phone.
- If the user does not know Z-PID or A-PID, then the user must log onto myid.msu.edu to retrieve number.
- Give number to HIT Technician.
- Log onto myid.msu.edu, verify number.
- If there is no Z-PID or A-PID for the account user, photo ID will be required.

HIT Technician