Samuel Lunenfeld Research Institute Information Technologies Department
Mount Sinai Hospital •Room 846 •600 University Avenue •Toronto ON M5G 1X5

Password Guide Summary.

The security features and procedures detailed below are intended as guidance. It is expected that only those security features or procedures appropriate for a particular environment would be expected to be implemented. Deviations from the guidance provided below and the rationale there for, however, must be documented in an organization's computer security program plan.

Security Features And Procedures.

1. **Automated Password Generation/Verification.** If employed, password generation or verification software should ensure that passwords are generated using those security features listed below which would be appropriate for a given site.
   1.1. Passwords contain at least eight non-blank characters.
   1.2. Passwords contain a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character.
   1.3. Passwords do not contain the user ID.
   1.4. Passwords do not contain any common English dictionary word, spelled forward or backwards (except words of three or fewer characters); dictionaries for other languages should also be used if justified by risk analysis.
   1.5. Passwords do not employ common names; that is, the password is checked against a set of common names to validate that the password does not contain any of the names, spelled forward or backwards (assuming that the name is over three characters).
   1.6. Passwords do not contain any commonly used numbers (e.g., the employee ID number, Social Insurance number, birth date, phone number) associated with the user of the password.
   1.7. Passwords do not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."

2. **User Selected Passwords.** In those cases where the user selects his/her own password (regardless of whether said password is verified by password verification software), the user should ensure that the selected password is consistent with those security features listed below that would be appropriate for a given site.
   2.1. Password contains at least eight non-blank characters, provided such passwords are allowed by the operating system or application.
   2.2. Password contains a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character within the first seven positions, provided such passwords are allowed by the operating system or application.
   2.3. Password does not contain the user ID.
   2.4. Password does not include the user's own or, to the best of his/her knowledge, close friends—or relatives—names, employee serial number, Social Insurance number, birth date, phone number, or any information about him/her that the user believes could be readily learned or guessed.
   2.5. Password does not, to the best of the user's knowledge, include common words that would be in an English dictionary, or from another language with which the user has familiarity.
   2.6. Password does not, to the best of the user's knowledge, employ commonly used proper names, including the name of any fictional character or place.
   2.7. Password does not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."
   2.8. Password employed by the user on his/her unclassified systems is different than the passwords employed on his/her classified systems.

3. **Password Integrity – Protection.**
   Individuals must not
   3.1. share passwords except in emergency circumstances or when there is an overriding operational necessity, approved by the SLRI IT;
   3.2. leave clear-text passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password;
   3.3. enable applications to retain passwords for subsequent reuse.

4. **Password Integrity – Changing.**
   Passwords must be changed
   4.1. at least every 6 months or every interval specified for particular application;
   4.2. immediately after sharing;
   4.3. as soon as possible after one suspects that a password has been compromised; and
   4.4. on direction from management.

5. **Administration.** If the capability exists in the information system, application, or resource, the system must be configured to ensure the following.
   5.1. Three failed attempts to provide a legitimate password for an access request result in an access lockout that will be automatically restored following a predetermined time period decided by the system manager. Alternative responses (e.g., by increasing the delay between attempts with each failure) to three failures to provide legitimate passwords for an access request (e.g., by increasing the delay between attempts with each failure) are also acceptable assuming such alternate responses are documented and approved by the SLRI IT.
   5.2. When a password specification does not comply with those requirements of 1.5. and 2.5. that are implemented, and if the failure to comply is verifiable by automated means, then the password specification is rejected.
   5.3. After 6 months (or interval specified for particular application) of use, individuals are notified that their passwords have expired and must be changed or lockout will occur.
   5.4. Any password file or database employed by the information system is protected from access by unauthorized individuals as technically feasible.

BY ORDER OF
SAMUEL LUNENFELD RESEARCH INSTITUTE
INFORMATION TECHNOLOGIES / INFORMATION SYSTEMS