

Legislative Services Agency (LSA)

Computer Network

Password Policy

Passwords are an important aspect of computer security. They are your front line of protection for electronic files and email accounts. A poorly chosen password may result in the compromise of the General Assembly's data and computer network operability. Computer hackers use sophisticated programs intent on gaining passwords. Once access has been achieved, malicious damage can be done to our files and website. Damaging email messages could be sent in the name of the General Assembly or through the names of specific Members and/or staff. As such, all LSA computer network users (including Members of the General Assembly, their staff and Legislative Council) are responsible for taking the appropriate steps to select and secure their passwords.

New Users

LSA must have a signed network Acceptable Use Policy form on file before assigning anyone a password to the LSA computer network system. Once this form has been signed, the Service Desk team will contact you by phone to assign you a temporary password. This temporary password can only be used once and must be changed the first time you login.

Password Expiration

All user-level passwords must be changed at least every 180 days. A notification email will be sent within ten days of the password expiration date. Failure to change your password before the expiration date will result in the inability to access the network. Should this occur, change your password immediately or contact LSA to receive a temporary password.

Password Security

If you suspect that your password has been compromised, change your password immediately and inform LSA. Members of the LSA Network Services staff can assist you in the easy process of changing your password from your office computer.

Do not give your password to legislative aides or pages! All passwords are to be treated as sensitive, confidential information. Passwords should not be written down. Passwords must not be inserted into email messages or other forms of electronic communication. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption. Should a member of the LSA staff need to work on your log-on

or troubleshoot with your password, you can and should create a new password when the work is finished. The LSA technician you're working with can help you change it.

Remember

- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't reveal a password to co-workers while on vacation

Password Selection Guidelines

Once the password has expired the user must choose a new, unique password. All user-level passwords must contain at least eight (8) characters and cannot be similar to the user name.

That is, the password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.

The new password must contain:

- One upper case
- One lower case
- One numeric character

In addition to the new criteria, it is strongly recommended that the following standards be used when choosing a password:

- Do not use any of the following characters: =+”/[|* ,?<>~
- Do not use a word that can be found in a dictionary
- Do not use a word in any language, slang, dialect, jargon, etc.
- Do not use personal information, names of family members or pets, birthdays, phone number, district information, etc.
- Passwords should never be written down or stored on-line.
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "tmb1w2r!" or "tmb!w@r" or some other variation. *NOTE: Do not use either of these examples as passwords!* For added password strength, you can add a space within your pass phrase. For example, "tmb1w 2r!"

Poor, weak passwords have the following characteristics:

- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - o Names of family, pets, friends, co-workers, fantasy characters, etc.
 - o Computer terms and names, commands, sites, companies,

hardware, software.

- o The words "senate", "house", "council" or any derivation.
- o Birthdays and other personal information such as addresses and phone numbers.
- o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- o Any of the above spelled backwards.
- o Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

If you are unable to log on to the computer network for any reason, contact the LSA Network Services staff at 212-4420.

Please direct questions and comments regarding this policy to Troy Pound, LSA Director at TroyPound@scstatehouse.gov or at 212-4420.