PASSWORD PROTECTION POLICY

Scope

This policy is an approved policy of the South Australian Little Athletics Association INC. Affiliated members of the association are required to adhere to this policy and are encouraged to adopt this at Centre level for the benefit of all members of the association.

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the South Australian Little Athletics Association (SALAA) resources. All users, including contractors and vendors with access to SALAA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on a quarterly basis.
- All production system-level passwords should be securely stored in a centralised, encrypted password safe database
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

Password Construction Guidelines

All users at SALAA should be aware of how to select strong passwords.

- Strong passwords have the following characteristics:
- Contain at least 3 of the four following character classes:
- Lower case characters
- Upper case characters
- Numbers
- “Special” characters (e.g. !@#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least eight alphanumeric characters.

PASSWORD PROTECTION POLICY

Weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

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 "Tmb1W>r~" or some other variation. =

(NOTE: Do not use either of these examples as passwords!)

Password Protection Standards

- Always use different passwords for various SALAA access needs whenever possible.
- Do not share SALAA passwords with anyone, including administrative assistants or secretaries.
- All passwords are to be treated as sensitive, confidential SALAA information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Chief Executive Officer.
- Always decline the use of the "Remember Password" feature of applications

If an account or password compromise is suspected, report the incident to the Chief Executive Officer

Users should not reuse the same passwords for other external systems (eg Facebook, LinkedIn, personal computers, etc.)

Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

PASSWORD PROTECTION POLICY

Use of Passwords and Passphrases for Remote Access Users

Access to the SALAA Networks via remote access is to be controlled using either a one-time password, authentication or a public/private key system with a strong passphrase.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by parties delegated to do so by the Board of Directors. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Authorisation

<Signature of the Chief Executive Officer>_____

<Date of approval by the Board>_____

For Further information on this document, please contact:

The South Australian Little Athletics Association INC.
Po Box 146 Torrensville Plaza, SA, 5031
Phone: (08) 8352 8133
Fax: (08) 8352 8155
Email: Office@salaa.org.au
Website: www.salaa.org.au