Microtrading
Your trusted IT partner

Sample password policy for sports governing bodies

Purpose

This policy describes a recommended set of requirements for a typical sporting body. It includes rules for password selection and maintenance, to maximise security of the password and minimise its misuse or theft.

Passwords are the most frequently utilised form of authentication for accessing information resources. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, passwords are very often also the weakest link in securing data. Password use must, therefore, adhere to the policy statement found below.

Scope

This policy applies to anyone accessing or using your network, cloud services or data. This use may include, but is not limited to, the following: personal computers, laptops and hand-held computing devices (e.g. mobile phones, tablets, USB memory keys etc) that access your corporate resources as well as your electronic services, systems and servers.

General policy

All passwords (e.g. email, web, application, desktop computer, etc) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity.

The strength of password should be aligned with the risks of data protection. Strong passwords and preferably alternative security measures, such as multi-factor authentication, should be used to secure your applications and systems. High risk systems include, but are not limited to: systems that provide access to critical or sensitive member information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

Data trustees and security administrators are expected to set a good example through a consistent practice of sound security procedures.

1. All passwords must meet the following minimum standards, except where technically infeasible:
    - be at least eight characters in length
    - contain at least one lowercase character
    - contain at least one number
    - contain at least one uppercase character
    - cannot contain your first name, last name, or username
2. To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password.
3. All passwords are to be treated as sensitive information and should therefore, never be written down or stored on-line unless adequately secured.
4. Passwords should NOT be inserted into email messages or other forms of electronic communication without the consent of the management team.
5. Passwords that could be used to access sensitive information must be encrypted in transit.
6. The same password should not be used for to access multiple services, applications, networks.
7. Individual passwords should not be shared with anyone, including administrative assistants or IT administrators, unless instructed by the management team.
8. If a password is suspected to have been compromised, it should be changed immediately, and the incident reported to the management team.
9. Penetration testing may be performed at any time with the authority of the management team.

Share accounts

In addition to the general password standards listed above, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

- Passwords for servers must be changed as personnel changes occur. If an account or password is suspected to have been compromised, the incident must be reported to your IT support team and potentially affected passwords must be changed immediately.
- Where technically or administratively feasible, attempts to guess a password should be limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
- Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimises clues that could result from hacker attacks.
- Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities, such as suspected attacks, should be reported to your IT support team.

Note: Log files should never contain password information.

Password examples

Poor	Strong	Stronger
Kitty	1Kitty	1Kitty$9
ilovepizza	1lovep1zza	!LoveP1zz4
Unit1983	Unit1983versity	Un!1983V3rsity

It's important for any organisation to maintain a good password etiquette.