

## MANAGING THE SECURITY OF SIS/INTEGRIS

A number of schools have not changed the SCHADM account password from the default setting when they first started using SIS. That means that dozens of people, many no longer working at the school know the SCHADM password and could access confidential data if they were to gain access to the school network.

Password protection is one of the most important principles of network, application and e-mail security. All SIS users are assigned a separate user ID and associated password for access to, and to provide security for the software and data.

A lack of strong password management practices could affect the integrity and security of the school SIS data leading to unauthorised access to, theft or corruption of student records, highly sensitive staffing information and/or financial fraud.

The Department has some very clear and easy to follow guidelines for maximising the security of data and workstations.

The Department recommends a number of basic security practices:

- Ensure your workstation or laptop is screen locked in your absence from your work area. This can be done by selecting and holding down the Ctrl, Alt and Del keys simultaneously. This will bring up the Windows Security Window. Select the Lock Computer button. This will lock the workstation until the Users password is re-entered.
- When leaving your work area for an extended period of time, including overnight, screen lock, log off or close down your workstation.
- Avoid changing passwords on a Friday, the last day of the week (or school term) or prior to public holidays because there will be a greater chance you will forget it by the next working day. Historically, Monday is usually the busiest day for the Customer Service Centre, mostly due to password resets.
- Common dictionary words are not to be used.
- if you cannot remember your password, it is acceptable to record a hint regarding your password such as a year, a number or maybe initials which indicate the version you are currently using. **Never write down and leave on display or secrete in an easily identifiable location your actual password/s or reveal what method you are using to generate your passwords.**

Ever lost your wallet or purse? Remember the sense of vulnerability you felt? The same applies when your password is stolen. Someone could be creating an online identity, opening new credit cards, applying for mortgages, chatting online disguised as you and you wouldn't know it until it was too late. Sometimes a strong password is the only barrier between hackers and a series of potentially harmful operations.

Users should note some DET applications require the first character of a password to be an alpha character. If you have difficulty changing your password and have a number as the first character, change it to a letter. If it still does not work, then call the Customer Service Centre on extension 5555 (internal) or 9264 5555 (external).

Stronger passwords could include:

- Upper and lower case; even stronger with special characters eg &, %, \$.
- Not contain easily identifiable personal information.
- Not use any part of the account identifier (username, login ID, etc).
- Meaningful to you.
- Kept secret.
- Changed every 30 days.

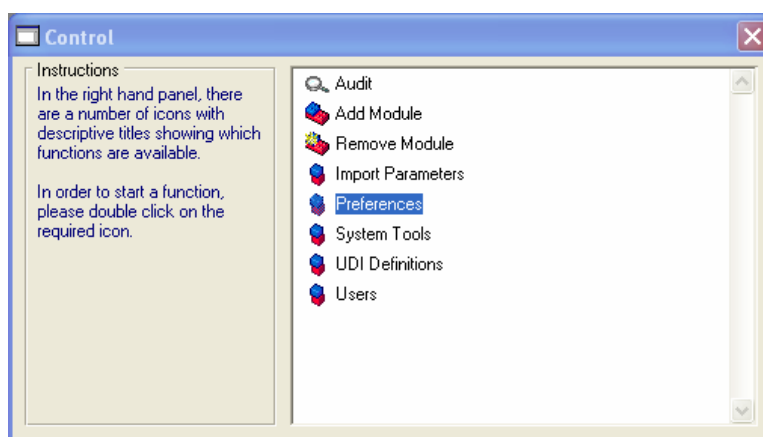
Having a sound method to version control your password is possibly one of the most important aspects of Password Management. Characteristics of an excellent method include the ability to:

- Update your password using completely new characters.
- Easily remember how the new password was generated.
- Carry out the process quickly.
- Use the same procedure in excess of twenty times without repeating the creation of a previous password.

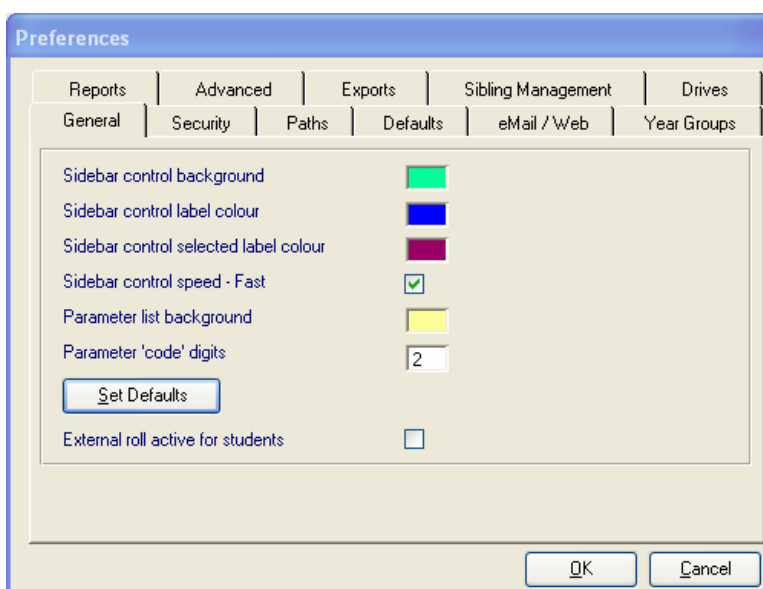
Some examples of ways in which a strong password can be generated are given at the end of this article.

Currently most schools have password security in SIS set to the minimum available. This can be improved to more closely meet DET standards in the following way:

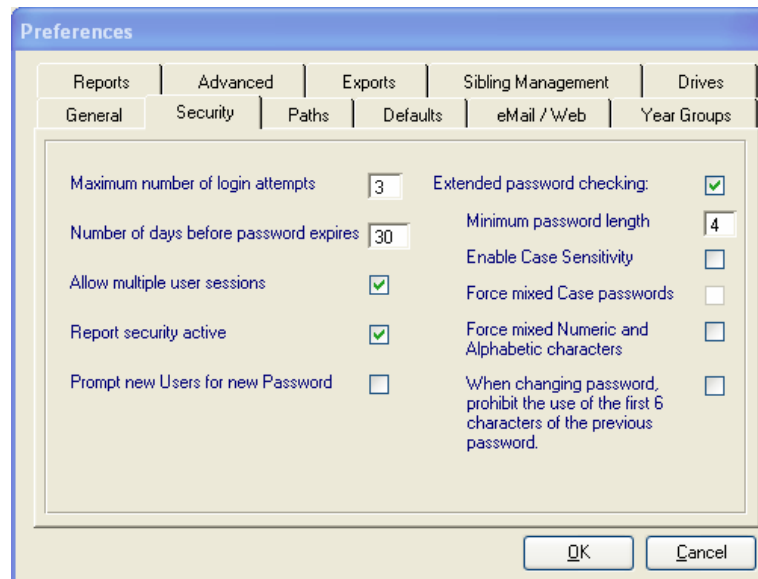
1. In the General Toolbar, select Control and Preferences.



2. Double Click on Preferences.



3. Select the Security Tab.



4. Select the following settings

- Change the *Maximum login attempts* to 5. This brings it in line with DET policy.
- Tick *Extended password checking*.
- Set the number of days before password expires to 30. This will require all users to change their password every 30 days and brings it in to line with DET policy.
- Set the minimum password length to 8. This will force users to use a reasonably hard to guess password and aligns it with DET policy.
- Tick *Enable Case sensitivity*. This will allow users to include capitals in their password.
- This will allow you to tick *Force mixed Case passwords*. This will require users to include at least one capital and one lower case letter in their password and brings it into line with DET policy.
- Tick *Force mixed Numeric and Alphabetic characters*. This requires users to use a mix of letters and numbers and aligns with DET policy.
- Tick *Prompt new Users for new password*. This will require users to change their password when they first log on to SIS in line with DET policy.
- Tick *When changing password, prohibit the use of the first 6 characters of the previous password*. This ensures that the User selects a different password each time.

5. Click on OK.

The following scenarios detail different strategies for creating strong passwords which can be customized to each user's situation. Keep your strategy for creating a secure password confidential.

**Passwords based on names or initials:**

- Select a family member or friend's initials and birth year (but not your own); Sarah Jessica Frazier Parker **sjfp**.  
Now include the year she was born **1962**.

New stronger password

**s1j9f6p2** or **19sjfp62**.

#### **Passwords based on an address:**

- Select an address of someone you know (but not your own);  
271 Alexander Parade, Dianella becomes **apd271** or **2apd71**.  
A stronger password would be **2aPd71** (combination of upper and lower case).  
Even stronger again would be **@2aPd71** (non alpha-numeric character included).

#### **Passwords based on songs.**

- Select a line from your favourite song or a song title.
- “Walking on sunshine” becomes **wos** or **Wos**.
- Add the four numbers of when the song was written – 1985.
- New stronger password is **19Wos85** or **1W9o8S5**.

#### **Passwords based on a phrase:**

- Pick a favourite phrase, one that means something to you.
- “Fool me once shame on you fool me twice shame on me”.
- Include numbers such as which letter you are selecting from each word to generate the password and the time of day when you created it.
- Therefore a new stronger password using the first letter of each word up to six letters would be “**fmosoy**” plus number of the letter you select, which is 1, and time you updated password. Hence “**1fmosoy1015**” is created.

#### **Passwords based on a succession:**

- Name the Australian Prime Ministers in succession or AFL Grand final winners. Also include the year when they were elected or won the premiership.
- George Houston Reid was the fourth Prime Minister from 18 August 1904 until the 5 July 1905; he was not a member of the Protectionist or Labour Party but stood for ‘Free Trade’. Hence **04GeRe05FT** is created.
- In 1990 Collingwood won the AFL Grand Final by defeating the Essendon. Therefore “**19ColEss90**” would be a VERY strong password.

#### **Next version based on names or initials:**

- Your existing password was **s1j9f6p2** or **19sjfp62** using the name Sarah Jessica Frazier Parker.
- When required to update your password select the next older or younger family member and once again include the year they were born.

#### **Next version based on an address:**

- Your existing password was **apd271** or **2apd71** using the address 271 Alexander Parade, Dianella.
- When required to update your password select the address of another family member or friend who lives further away.

#### **Next version based on songs.**

- Your existing password was **19Wos85** or **1W9o8S5** from the song title “Walking on sunshine” written in 1985.

When required to update your password select the next song title from the album.

#### **Next version based on a phrase:**

- Your existing password was **1fmosom1015** from the phrase; “Fool me once shame on you fool me twice shame on me”.

When required to update your password select the next letter in the sequence and the new time when you updated your password.

**Next version based on a succession:**

- Your existing password was 04GeRe05FT or 19ColEss90 which was determined by previous Prime Ministers or AFL Grand Final Winners.

When required to update your password select the name and year of the following Prime Minister or the next AFL Grand Final winner in 1991.