Risk Information – Churches
Cyber Series - Passwords

Passwords represent the most common way of protecting resources and activity when using a computer. Passwords can be used to access a program or data. They can be used to conduct on-line banking and access other on-line functions.
Protection of passwords is a critical component in maintaining the integrity of your church computers and networks.

The information provided in this publication is intended to assist churches understand the need to create, maintain and use passwords.

Keeping your passwords secure is a key strategy to maintaining the integrity of your computers and networks.

Passwords should be changed on a regular basis; we recommend a minimum of quarterly for functions with lower levels of risk or monthly where the risk is higher. Where possible, use computer based features to force password changes at the required interval.

Change default passwords the first time you use an application or hardware or software components. Do not leave default passwords unaltered.

Don’t share passwords; if guest passwords are used, limit the functionality that can be undertaken using them. Internal policies / practices should stress the importance of password confidentiality to all users; HR practices should include sanctions for disclosing passwords.

Do not provide your password to anyone in response to requests over the phone or via email or messaging service.

Do not write down passwords.

Change passwords if there is any doubt as to whether they have been compromised.

Do not make passwords obvious.

Follow the following principles for establishing your passwords:

- Minimum of 8 characters
- Mix of upper and lower case letters, numbers and special characters (at least one of each)
- Do not use words or names associated with the user
- Do not use numbers associated with the user (e.g. Birthday)

The information provided is of a general nature only and may not identify all matters that need to be included in the design of effective controls for the subject area. Professional advice should be obtained on individual circumstances.

Risk Information – Churches
Cyber Series - Passwords

Where possible use 2 factor identification. This form of identification requires the use of a password and some other information provided to the user, such as a code sent to the user's mobile phone that the user must enter to the application to complete the sign-on process.

When using internet banking services for (church) business purposes always require 2 people to action payments (use of bank provided tokens is recommended). It is recommended that all access to online financial services be closely monitored to enable timely identification of any unauthorised access.

Be extremely careful when using public computers (e.g. in an internet café) or when accessing the internet when you do not know how access is secured: do not attempt to access secure data or functions as the security of these computers may have been compromised.

When data is removed from church servers or networks on portable devices, e.g. on iPads, laptop computers or memory sticks, we recommend that access to data be password protected and/or encrypted.

The information provided is of a general nature only and may not identify all matters that need to be included in the design of effective controls for the subject area. Professional advice should be obtained on individual circumstances.