POLICY HR 06

Electronic Security

Description

The work and ministry of the Presbytery requires electronic devices to be connected to key Presbytery data sources. Using such equipment and methods opens the Presbytery and those the Presbytery serves; to potential e-security risks.

Applicability

This policy applies to all who gain access to any level of information as a representative of the Presbytery.

It applies to all devices regardless of the ownership or physical work location.

Policy

1. **Log ins;**

   It is expected that where a login is required the following expectations should be met:

   a. Login details should be updated on a regular basis

   b. Login should not be deemed "weak" by best practice standards

   c. Login details should not be shared with others, unless there is approved access. The shared access should be revoked after the work is complete

   d. Log in details are to be updated should there be concern of a breach, or potential breach of security; and

   e. When available, select 'double authentication' log in methods

2. **Anti-virus;**

   It is expected that each device used for the work of the Presbytery has an up to date and functioning Anti-Virus software.

   Scans are to be run regularly to reduce the risk of attack.

3. **Back up information**

   Unless a paid cloud storage system is used, data is to be backed up to a secure external hard drive at least every six (6) months.

Document Control

Update Prepared by		Ian Goff
Date issued		24 May 2022
Endorsed by		Kent Crawford
Tabled		Standing Committee 28 April 2022
Version N#		.02
Edits from prior version		Minor edits and updated for improvements in technology
Policy N#		HR06