**Cybersecurity Self-Assessment
for Non-Profits**

1. Cybersecurity only relates to protecting personal or sensitive electronic information.

- ○ True
- ○ False

2. Who is ultimately responsible for a charity's cybersecurity?

- ○ The head of IT or Chief Information Officer
- ○ The Chief Executive Officer
- ○ The charity's Responsible Persons (its board or committee members)

3. What is the first thing a charity should do to identify cybersecurity risks?

- ○ Install a firewall for its network
- ○ Consider the information it holds that could be valuable to an attacker and prioritise its protection
- ○ Ensure individuals have strong passwords on their work devices, including computers and phones
- ○ Revoke access to the internet for part-time staff and volunteers

4. Moving to the cloud takes care of cyber security as it is now the vendor's responsibility.

- ○ True
- ○ False

5. Small charities are less vulnerable to cyberattacks than large corporations or government agencies.

○ True
○ False

6. What should a charity do if it identifies a data breach?

○ Follow the Office of the Australian Information Commissioner's guidance on data breach preparation and response
○ Contact the ACNC to notify of the breach
○ Replace the device or system that led to the breach occurring
○ Reprimand the person responsible

7. Of the following, select the cybersecurity risks

○ A trusted, long-time charity employee having unauthorised access to files they shouldn't have access to.
○ Sending new volunteers to a cybersecurity training session before they start work with the charity.
○ Clicking on a link in an email from an unfamiliar source to see if its contents are legitimate
○ Having a shared password for a shared charity computer written down on a notepad next to the computer.

8. Select the correct option to complete the sentence. A charity shouldn't...

○ Keep a written register of the passwords for its critical assets
○ Store back-ups of important information in the 'cloud'
○ Publicly acknowledge a data breach if it occurs
○ Use a two-step process for logging in to a computer or device
○ Issue devices such as tablets and phones to part-time staff or volunteers