BRISBANE NORTH

An Australian Government Initiative

Service provider information security assessment

Information security systems protect an organisation's most important assets, it protects the accessibility, confidentiality and integrity of the systems, data and applications used.

This assessment has been issued by Brisbane North PHN (PHN) to serve as an assessment of the information security controls used by your organisation. The protection of personal and sensitive data is critical. The answers provided in this assessment will help the PHN to make a decision as to the level of Information Security controls used by your organisation. Any deliberate false answers on this assessment could be treated as a breach of contract or disqualify you from tendering for services.

Service Provider details	
Company name:	
Assessment completed by:	
Contact details	
Date of assessment	

Service Provider Information Security Assessment	Yes / No
1. Anti-Malware / Anti-Virus software protects computers from malicious attacks such as computer viruses, worms, Trojan horses, ransomware or spyware. Are all your organisations computers, including servers protected with Anti Malware / Anti-Virus software?	
2. Security patches are released by software providers to correct and prevent specific vulnerabilities. Are all security related patches applied immediately, including Operating Systems (Windows, MAC), Applications (such as Word, Excel, Adobe, Anti Malware, Anti-Virus) and Internet Browsers?	
3. Firewalls help protect networks by filtering traffic and blocking outsiders from gaining unauthorised access to private data. Do you have a Firewall in operation to ensure that only authorised network traffic is permitted?	
4. Passwords are the first line of defence against unauthorised access to your computers and personal information. Do your staff use strong passwords and do not share their login credentials with others?	

5. Common cyber security threats include computer viruses, unauthorised access or Phishing emails that trick users in providing personal information and can include requests for money, bank account changes, opening malicious attachments or requests to provide user login details. Your staff are made aware of Cyber security threats such as Phishing emails and know what to do if they receive one?	
6. Do you have a clearly defined process to report a suspected or actual data breach?	
7. Your staff understand patient confidentiality when accessing client information systems, including access in public places?	

Please ensure you have answered all the questions correctly with either a Yes or No. If you have additional comments to add please include the here:

Useful resources for Cyber and Information Security can be found at these sites:

- Australian Cyber Crime Centre (ACSC)
- Essential Eight
- Protective Security Policy Framework (PSPF)
- Cyber Security Principles
- Notifiable data breach
- Australian Charities and Not-for-profits commission – Cyber Security