PEXA Technical Requirements

Class 1 & 2

"Integrator" means the party to an integration agreement with PEXA.

1. **Security Training and Awareness Programs**

   (a) The Integrator must provide staff with cyber security training.

   (b) The Integrator must ensure that staff are aware of potential cyber security threats as it relates to the PEXA APIs and the PEXA Platform.

2. **Information Security Policy**

   The Integrator must maintain an information security policy that governs staff practices around IT security. The policy should align to the information security management system (ISMS) standard where possible given the nature and size of the organisation.

3. **Firewalls**

   The Integrator must maintain a firewall policy on servers and endpoint devices; securing the incoming and outgoing traffic, and monitoring and alerting of breach attempts.

4. **Anti-Malware/ Virus Scanning Processes**

   The Integrator must regularly perform anti-malware/virus scanning and resolve any issues that are reported.

5. **Patch and Vulnerability Management**

   (a) The Integrator must have installed the most recent patching releases.

   (b) The Integrator must regularly scan for vulnerabilities.

   (c) The Integrator must have a formal process to categorise known vulnerabilities based on severity (i.e. high, medium and low).

   (d) The Integrator must prioritise high and medium vulnerabilities for patching.

6. **Transport Layer Security**

   The Integrator must maintain the Transport Layer Security (TLS) version advised by PEXA.

7. **No Multiple Workspace Activity**

   The Integrator must prevent Multiple Workspace Activity.