Zedmed best practice guide

Last Modified on 20/10/2023 3:37 pm AEDT

Zedmed software is a critical part of our customer's service delivery, and when a **Zedmed server is on-site,** it should be operated as part of a best-practice IT strategy. This document lists key best practice considerations and links to Australian healthcare industry guidance.

> Zedmed strongly recommends that qualified technicians and providers manage your information systems and security.

Backups

- The server that Zedmed is installed on should be backed up daily.
- The backups should be stored in a safe place and tested to ensure they can recover your systems.
- The backup schedule should include a rotation of weekly, monthly, and annual backups, stored offsite.
- There should be a Disaster Recovery Plan and an annual test of this plan.

To learn more, see the backup guidance provided bythe Australian Health Agency and digitalhealth.gov.au

Software

- Servers and desktops running Zedmed software must use operating systems supported by Zedmed.
- Servers and desktops should have the latest Windows updates and patches.
- Internet browsers and applications should have the latest patches and security updates.

To review Zedmed's hardware and software requirements, see the Zedmed Specifications document.

Security

- Antivirus software should be installed on all servers, workstations and devices connected to the practice.
- Firewalls should be used to control connections in and out of all practice sites.

To learn more, see the RACGP computer and information security standards.

Staff

- Staff should only have the Widows and Zedmed access required to perform their role.
- Staff should have security awareness training that covers social engineering, malware and phishing.

To learn more, see the Digital Health Cyber security awareness resource.