RACGP | *Business continuity/redundancy*

With the increasing dependence on electronic information systems and access to information, having a business continuity plan contributes to good governance processes within a practice. Management and recovery from a computer malfunction or security incident needs to be planned for. Here are some things to consider if your hardware or software is affected, along with a number of useful links.

Data management

To ensure the continuous operation of your practice it is critical to have a plan for how you store, backup and archive your practice data.

For more information, refer to the RACGP's Computer and information security standards (CISS) Standard 7 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-7/

For a computer security checklist and videos on the CISS topics, refer to the RACGP's Digital Business Kits at www.racgp.org.au/digital-business-kit/ciss-checklist/

Mission critical

It is important to have a plan as to how you would keep your business running if something goes wrong, eg. natural disasters or power failure.

For more information, refer to the CISS Standard 2 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-2/

For a computer security checklist and videos on the CISS topics, refer to the RACGP's Digital Business Kits at www.racgp.org.au/digital-business-kit/ciss-checklist/

For a series of templates on disaster recovery refer to the RACGP Emergency Response Planning Tool https://erpt.racgp.org.au/standardlogin

Redundancy

In computing, this refers to duplicate devices that are used for backup and failover, ie. it is essential to have multiple mission-critical devices so information can still be accessed in case one fails.

For more information, refer to the CISS Standard 7 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-7/

For a computer security checklist and videos on the CISS, refer to the RACGP's Digital Business Kits website at www.racgp.org.au/digital-business-kit/ciss-checklist/

Emergency management and disaster recovery

Practices should have a strategy on how to prepare for, respond to and recover from the impacts of emergencies and pandemics. The RACGP has an Emergency Response Planning Tool (ERPT) to help practices develop a strategy for emergency management.

For a series of templates on disaster recovery, refer to the RACGP's ERPT at https://erpt.racgp.org.au/standardlogin

.

Business continuity/redundancy in general practice checklist

Date of completion

Name of practice

Our practice has a business continuity plan which includes a process for managing and recovering from a computer malfunction or security incident. We have considered the following items when developing our business continuity plan and consulted with an IT professional on any further recommendations.

- [ ] Data management
- [ ] Mission-critical
- [ ] Redundancy
- [ ] Emergency management and disaster recovery

Notes