Macquarie Data Centres. Seriously Secure.

SOC 2: It's about trust and information integrity.

A SOC 2 audit is an audit of a service organisation's non-financial reporting controls as they relate to the Trust Services Criteria:

- Security
- Confidentiality
- Privacy
- Availability
- Processing Integrity

Why is SOC 2 important?

A SOC 2 audit report provides user entities such as our valuable Data Centre customers with the assurance and peace of mind that the non-financial reporting controls are suitably designed, in place, and appropriately protecting sensitive client data.

How many audits are there?

There are two audit reports.

SOC 2 Type 1

An attestation of controls on the data centre at a specific point in time.

SOC 2 Type 2

An attestation of controls at a data centre over a minimum six-month period.

SOC 2 Type 1 Report.

The SOC 2 Type 1 reports on the description of controls provided by management of the service organisation and attests that the controls are suitably designed and implemented.

SOC 2 Type 2 Report.

The SOC 2 Type 2 reports on the description of controls provided by management of the service organisation, attests that the controls are suitably designed and implemented, and attests to the operating effectiveness of the controls.

AICPA Trust Services Principles & Criteria.

Security

- Two-factor authentication
- Intrusion detection
- Network/application firewalls

Confidentiality

- Encryption
- Access controls
- Network/application firewalls

Availability

- Performance monitoring
- Disaster recovery
- Security incident handling

Privacy

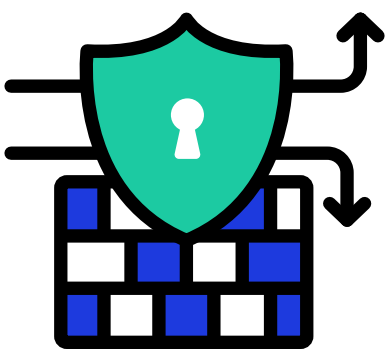
- Access control
- Two-factor authentication
- Encryption

Processing integrity

- Quality assurance
- Processing monitoring

How is it relevant?

Vulnerability assessments and penetration tests are generally used in SOC Type II audits to test the effectiveness of the controls implemented by an organisation.



Visit macquariecdatacentres.com to learn more about how seriously we take security.

macquarie DATA CENTRES