Digital Infrastructure
INSTITUTE

COMMUNITY INFORMATION SHEET

Cyber & data security

How data and critical infrastructure are protected

What's the concern?

Data centres hold and process information, and are part of the nation's critical infrastructure. People ask how data is kept private and secure, how the facility itself is protected from cyber and physical threats, and whether sensitive data stays in Australia.

The facts

Operators are subject to privacy law and recognised information-security standards, and large facilities fall under national critical-infrastructure and cyber-security obligations. Good practice includes strong physical security (hardened perimeters, access control, monitoring), cyber resilience, and — for government and community data — appropriate data residency and sovereignty so sensitive information is protected and, where required, kept onshore.

What good practice looks like

- Compliance with privacy law and recognised information-security standards (e.g. ISO/IEC 27001).
- Strong physical security and cyber resilience, consistent with critical-infrastructure obligations.
- Appropriate data residency and sovereignty for government and community data.
- Independent assurance of security arrangements, with access limited to those with a right to it.

Questions you can ask

- What standards govern the facility's data and cyber security?
- Where is sensitive data stored, and does it stay in Australia?
- How is physical access to the site controlled?

Want to know more? Your local council, the EPA Tasmania and ARPANSA publish further information. This sheet is general information, not medical, legal or planning advice; figures are indicative and a specific proposal is confirmed by qualified assessment.