ACSC — Ransomware: First 24 Hours (Guidance Extract)

This document summarises immediate actions for organisations responding to ransomware.

Immediate actions (first 24 hours):
1. Contain affected systems and isolate where necessary.
2. Preserve logs and volatile evidence.
3. Establish an incident management structure and comms lead.
4. Identify critical business services impacted.
5. Engage external support (IR, legal, comms) as required.
6. Consider notification obligations and stakeholder engagement.

Operational security:
- Assume attacker monitoring of public statements.
- Avoid confirming scope until assessment is complete.
- Use consistent language across stakeholders.

Date: 2026-03-21 (Simulation)