

Southern Ports is committed to the privacy of its stakeholders and takes reasonable steps to reduce the potential for an information breach. An information breach occurs when there has been unauthorised access or loss of information managed by Southern Ports or its authorised partners.

This Policy outlines the mandatory requirements to identify, respond and manage an information breach at Southern Ports and reinforces Southern Ports commitment to responsible information handling.

This Policy applies to all Southern Ports employees, Board members, contractors, volunteers, and third parties who handle information on behalf of Southern Ports.

POLICY STATEMENT

Southern Ports, as an Information Privacy Principle entity, is committed to:

- reducing the likelihood of information breaches.
- implementing measures to safeguard the data and information it collects, manages, uses, and discloses as part of its functions and activities.
- developing and embedding processes that define what a breach is, how breaches are managed, the roles and responsibilities, and the management of related artefacts.
- complying with all legislative, regulatory, and contractual obligations related to data handling, privacy and security.
- detecting and responding promptly and effectively to any information breach.
- reporting to relevant authorities any suspected data breaches immediately.
- reviewing all incidents to mitigate harm and prevent future incidents.
- participating in regular training on data protection and breach response procedures.
- managing and enhancing Southern Ports information management systems to ensure effective information security management.

RATIONALE AND EXPECTATIONS

This commitment aligns with the Office of the Australian Information Commissioner's Notifiable Data Breaches Scheme and the WA Government Office of the Information Commissioner in accordance with the Privacy and Responsible Information Sharing legislation.

This Policy's approach is consistent with the WA Government Cyber Security Policy and Cyber Security Incident Response and Coordination Framework, together with [Southern Ports Privacy Policy](#) and relevant subject documents.

This policy does not apply to information accessed under the Freedom of Information Act.

For questions or concerns about this Policy, please email privacy@southernports.com.au.

REVIEW AND UPDATE

A review of the effectiveness and relevance of the Policy will be conducted at least every two years on the anniversary of the effective date of the Policy unless there is a material change which affects the intent of the Policy.

Approved by the Board on 20 August 2026.