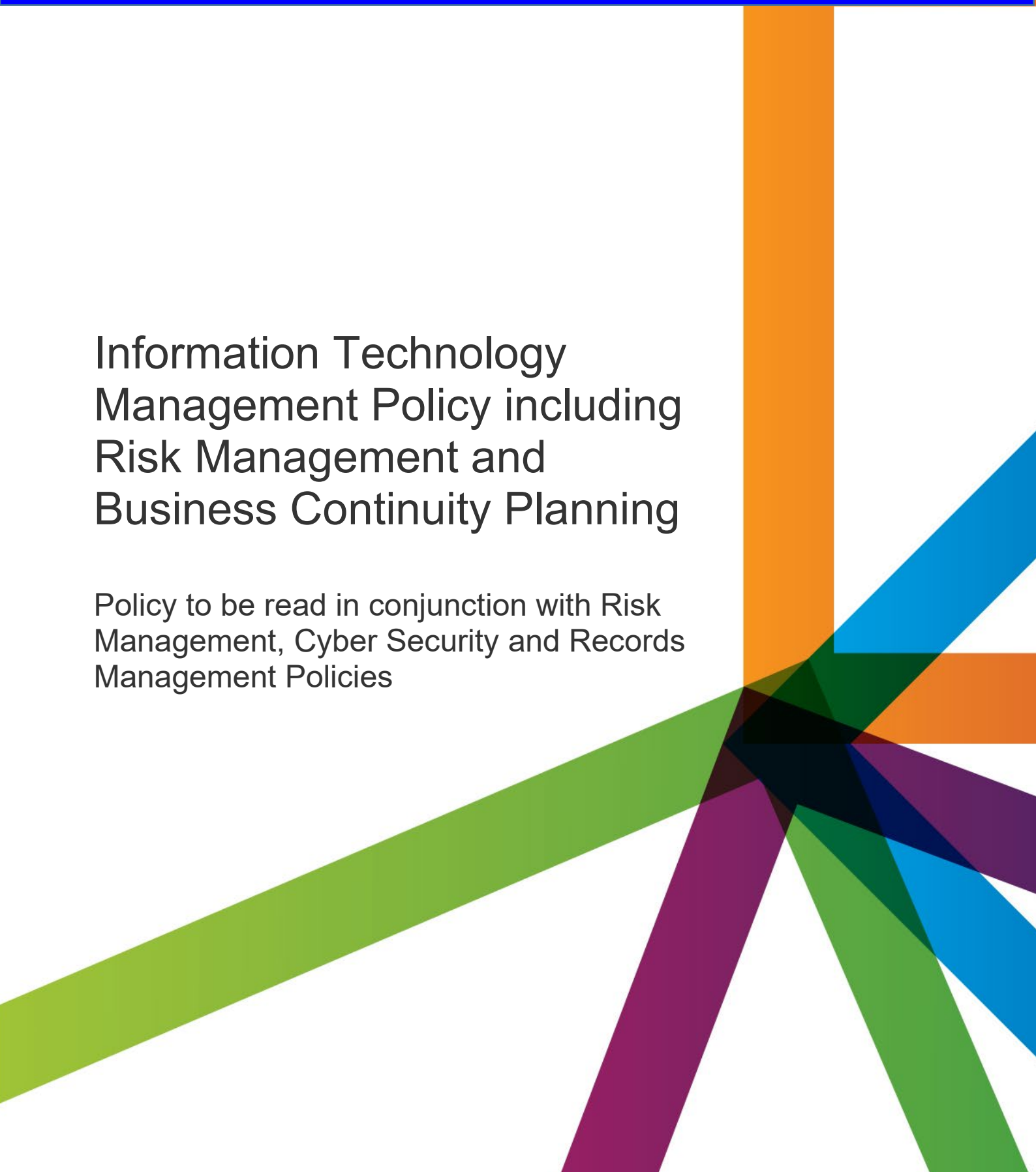


Illawarra Shoalhaven Joint Organisation Policy Manual

Information Technology Management Policy including Risk Management and Business Continuity Planning

Policy to be read in conjunction with Risk
Management, Cyber Security and Records
Management Policies



1. Policy Statement

The Illawarra Shoalhaven Joint Organisation (the ISJO) adopts Business Continuity Management as a core obligation of good governance.

The ISJO recognises that Business Continuity is an integral part of good management practice and fully supports Business Continuity Management as an important element in its Risk Management Framework. The purpose of this Policy is to clearly document our commitment to recognising the importance of business resilience and long-term performance most especially in regard to Information Technology and Data access.

This Policy protects the interests of the ISJO and its stakeholders by employing a rigorous process for the effective management and mitigation of potential disruption risks to our business functions and to identify resources and capabilities required to ensure the uninterrupted availability of all key resources necessary to support those functions during an outage.

2. Purpose

The purpose of our Policy is to:

- Maintain the highest possible integrity and continuity for services provided by our organisation
- Safeguard our assets including data and financial resources
- Plan for the uninterrupted availability of resources so that the ISJO can continue to perform the business functions that support its critical objectives
- Ensure that the ISJO can appropriately deal with any disruption and restore operations as soon as practicable
- Demonstrate responsible Business Continuity Management processes that align with applicable best practice standards and methods, and
- Support the accurate and timely provision of information to staff, business partners, stakeholders and other relevant levels of Government during an outage event.

3. Procedures, Standards and Protocols

The ISJO has contracted an external provider to provide access to Cloud storage and ongoing service assistance including and especially assistance required as a result of a critical breakdown in technology access (whether disaster related or otherwise).

Core services within our service agreement include:

IT service and support on an ongoing basis

- Work flows and work issues are filtered via a site contact to allow awareness of issues as they arise
- Remote Assistance is provided and Add/Move/Change tasks can be undertaken remotely
- Business Hours Access and escalation / On Call is available 24 hours a day / seven days a week
- Systems Documentation access, support and review is ongoing.

IF PRINTED THIS MAY NOT BE THE CURRENT VERSION

See shared drive for the most recent version of this document

Document	Information Technology Business Continuity	Author:	Roger Stephan	Approved by:	Chief Executive
Date:	10 June 2025	Review Date	Annually on 30 June	Doc ID:	
Version:	1	Amendment notes:			

Server / Desktop Support tools

- Remote Support Access capacity available 24 hours a day / seven days a week
- Desktop Maintenance / Asset / Reporting information provided on an ongoing basis
- Automated Windows Desktop Patching services and reporting provided on an ongoing basis
- Platform provided to provide other optional services like Web Content Filter, Managed Antivirus, etc.

Server Monitoring and Preventative Maintenance

- Remote Support Access available 24 hours a day / seven days a week
- Server Monitoring and Alerting Services (e.g. Backups, System Health, Event Logs, Data Growth, Services Stability, etc.) is available 24 hours a day / seven days a week
- Automated Server Patching and Reporting is in place 24 hours a day / seven days a week
- Alerts during business hours actioned via Service Desk.

Disaster Recovery

- All ISJO data is backed up daily to the Cloud and remotely. Backups are monitored daily and servers constantly maintained to ensure quick recovery from critical incidents
- Our provider's Partner Program offers SLAs to ensure our organisation confidence in the event a disaster occurs
- Weekly antivirus updates are included and include tools to minimise malware, SPAM and ransomware attacks
- Backups are constantly monitored and any issues will be reported to the ISJO on discovery.

Asset / Equipment Integrity

- All information technology equipment including laptops and mobile devices must be capable of accessing our central systems including platforms and software. Any equipment that is obsolete / cannot be updated / cannot connect to our core operating system (currently Windows 11) must be disposed of in accordance with our Asset Acquisition and Disposal Policy and replaced at the relevant program's cost by appropriate equipment.

Document Integrity

- To mitigate against loss caused by disaster events, and to facilitate conformity with information access requirements under the [Government Information Public Access \(GIPA\) Act 2009](#), work related files must be saved – in accordance with our Records Management Policy – to the ISJO's OneDrive. ISJO documentation / files must not be saved exclusively to laptop hard drives. It should be noted, in that regard, that remote access to the ISJO OneDrive is enabled through work laptops. Saving to hard drives is therefore not operationally required or desirable.

IF PRINTED THIS MAY NOT BE THE CURRENT VERSION

See shared drive for the most recent version of this document

Document	Code of Business Ethics	Author:	Roger Stephan	Approved by:	Chief Executive
Date:	30 November 2024	Review Date	Annually on 30 June	Doc ID:	
Version:	1	Amendment notes:			