Disaster Recovery Plan (IT Services) Policy & Procedures

1. Purpose

To ensure that Nepean Community College (NCC) can **restore IT systems, data, and services** following a disruption, minimising impact on:

- Student learning and delivery (e.g. LMS, DSEC systems)
- Financial and compliance systems (e.g. invoicing, funding reporting)
- Data security and privacy obligations

This supports continuity objectives already identified in NCC planning frameworks.

2. Scope

This policy applies to:

- All IT systems (on-premise and cloud)
- Student management systems (aXcelerate)
- Learning platforms (Catapult)
- Financial systems (Xero)
- Email and communications platforms (Microsoft Office systems)
- Third-party hosted services (Amity IT & Tresami)

3. Policy Statement

NCC will:

- Maintain **secure backups** of critical systems and data through a third-party arrangement off-site with Tresami
- Ensure **rapid restoration capability** following a disruption
- Test disaster recovery processes annually
- Align IT recovery with broader **business continuity and critical incident management plans**

4. Key Principles

- **Availability** – Systems must be restored within acceptable timeframes
- **Integrity** – Data must be accurate and complete
- **Confidentiality** – Data breaches must be avoided during recovery
- **Compliance** – Must meet Privacy Act 1988, RTO Standards 2025 (ASQA)/NESA requirements and cyber insurance guidelines

5. Disaster Scenarios Covered

- Cyber attacks / ransomware
- Data loss or corruption

- System or server failure
- Cloud provider outage
- Power failure or physical site damage
- Loss of internet connectivity

6. Critical Systems Classification

Priority Level	System Type	Example
Critical (24–48 hrs)	Student, finance, LMS	SMS, Xero, LMS
Important (2–5 days)	Admin systems	Email, SMS
Non-critical	Archive systems	Legacy data

7. Roles and Responsibilities

CEO

- Overall accountability
- Approves disaster declaration
- External communication (stakeholders, media)

Tresami IT Provider / IT Lead

- Leads technical recovery
- Oversees system restoration and validation
- Conducts root cause analysis

Administration

- Communicates with students and staff
- Coordinates manual processes (if required)

Incident Response Team

- Coordinates overall response and escalation
- Aligns with existing incident response structure

8. Backup Strategy

NCC (through Tresami) will maintain:

- Daily backups of:
    - Student data
    - Financial data
    - LMS content

- Offsite/cloud backups
- Multiple backup versions
- Secure access controls

Backups must be:

- Tested periodically
- Stored in a separate environment

(This aligns with our existing requirement for regular data backups and recovery capability).

9. Disaster Recovery Procedures

9.1 Detection & Declaration

- Identify incident (system failure, cyber incident, outage)
- Assess severity and impact
- CEO or delegate declares disaster if required

9.2 Initial Response

- Activate Incident Response Team
- Isolate affected systems (if cyber-related)
- Notify IT provider immediately

9.3 System Recovery (Core Steps)

1. Identify impacted systems
2. Prioritise based on criticality
3. Restore from backups
4. Rebuild systems (if required)
5. Apply security patches
6. Validate system integrity

9.4 Data Recovery

- Restore latest clean backup
- Verify data integrity
- Confirm no corruption or malicious code

9.5 Testing & Validation

- Confirm:
    - System functionality
    - User access
    - Data accuracy

- Conduct security checks

9.6 Communication

- Internal:
  - Staff updates (status, timelines)
- External:
  - Students and stakeholders (if service impacted)
  - Regulators if required under Privacy Act, ASQA etc.

9.7 Return to Operations

- Resume normal service delivery
- Monitor systems closely
- Implement interim controls if needed

9.8 Post-Incident Review

- Document:
  - Cause of incident
  - Response effectiveness
  - Lessons learned
- Update DR plan and controls

10. Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO)

System	RTO	RPO
SMS / Student Systems	24–48 hrs	≤ 24 hrs data loss
Finance Systems	24–48 hrs	≤ 24 hrs
LMS	24–72 hrs	≤ 24 hrs
Email	24 hrs	≤ 12–24 hrs

11. Testing and Review

- Annual disaster recovery simulation
- Testing after major system changes
- Results reported to College Council

12. Training and Awareness

- Staff training on:

- Email, security 7 phishing
- Incident reporting
- System access procedures

- IT provider training on recovery protocols

---

13. Compliance Requirements

This plan supports:

- Privacy Act 1988 (data protection)
- RTO Standards (records and data security)
- NESA alternative education program requirements
- Cyber insurance obligations (noted in your insurance documentation)

14. Related Documents

- Incident Response Plan (IT)
- Continuity Checklist Plan
- Crisis Response Policy
- Data Breach Response Plan

15. Policy Review

- Review annually
- Review after any significant incident
- Approved by College Council