INCIDENT DATA RESPONSE PLAN

1. Purpose

The purpose of this Incident Data Response Plan is to establish a structured approach for responding to data breaches, ensuring swift and effective actions to mitigate impact, restore normal operations, and comply with legal and regulatory requirements.

2. Scope

This plan applies to all incidents involving unauthorised access, use, disclosure, alteration, or destruction of sensitive data at Nepean Community College.

3. Incident Response Team (IRT)

- **Incident Response Manager**: Oversees the response efforts and coordination, this will be the CEO.
- **Information Security Officer (ISO)**: Leads the technical response and investigation, this will be an external IT provider.
- **Legal Counsel**: Provides legal advice and ensures compliance with regulations.
- **Communications Officer**: Manages internal and external communications, this will be the CEO.
- **IT Support**: Provides technical assistance and support during the response, this will be the external IT provider.
- **Affected Training Representatives**: Represent the interests and concerns of the affected areas.

4. Steps in Case of Data Breach

4.1. Preparation

- **Training and Awareness**: Regularly train staff on data breach prevention, detection, and response.
- **Incident Response Drills**: Conduct periodic drills to test and improve the response plan.
- **Documentation**: Maintain up-to-date documentation of the Incident Data Response Plan.

4.2. Identification

- **Detection**: Monitor systems for signs of potential data breaches, such as unusual login activities, unexpected data access, or alerts from security tools.

- **Reporting**: Encourage immediate reporting of suspected breaches by any employee, contractor, or student to the ISO.

4.3. Containment

- **Immediate Response**: Isolate affected systems to prevent further unauthorised access.
- **Short-term Actions**: Disable compromised accounts, change passwords, and apply security patches.
- **Long-term Actions**: Implement additional security measures as needed to secure the environment.

4.4. Eradication

- **Investigation**: Conduct a thorough investigation to identify the root cause of the breach.
- **Removal**: Eliminate malicious code, unauthorised access points, and other threats from the systems.
- **Validation**: Ensure that the systems are clean and secure before resuming normal operations.

4.5. Recovery

- **Restoration**: Restore affected systems and data from clean backups.
- **Testing**: Test the restored systems to ensure they are functioning correctly and securely.
- **Monitoring**: Continue to monitor the systems for any signs of residual issues.

4.6. Notification

- **Internal Notification**: Inform key stakeholders, including management and affected departments, about the breach.
- **External Notification**: Notify affected individuals and regulatory bodies, such as the Office of the Australian Information Commissioner (OAIC), as required by law.
- **Public Communication**: Prepare public statements if necessary, ensuring transparency and maintaining trust.

4.7. Lessons Learned

- **Post-Incident Review**: Conduct a review meeting to analyse the incident and response efforts.
- **Documentation**: Document the incident, response actions, and lessons learned.

- **Improvement**: Update the Incident Response Plan and security measures based on insights gained from the incident.

5. Compliance and Legal Considerations

- **Legal Obligations**: Ensure compliance with relevant laws, such as the Privacy Act 1988 (Cth) and the Notifiable Data Breaches (NDB) scheme.
- **Regulatory Reporting**: Report the breach to regulatory bodies as required.

6. Policy Review and Update

- **Annual Review**: Review and update the Incident Response Plan annually or as needed.
- **Communication**: Communicate updates to all relevant stakeholders.