POLICY TITLE:	Information Security Policy

1. Policy Statement and Purpose

The purpose of the Information Security policy is to protect the confidentiality, integrity, and availability of Chris O'Brien Lifehouse (COBLH) information assets from unauthorised access, use, disclosure, destruction, and alteration. The policy safeguards the reputation of the organisation and ensures that workforce members, including management of COBLH's information and information systems meet IT security and data protection requirements.

2. Policy Scope

This policy applies to all users of all information systems that are the property of COBLH and its patients. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by COBLH.
- All contractors and third parties that work on behalf of and are paid directly by COBLH.
- All contractors and third parties that work on behalf of COBLH but are paid directly by an alternate employer.
- All employees of partners and clients of COBLH that access COBLH's non-public information systems.

3. Definitions

Target State for Information Security - The desired and planned level of information security maturity that an organisation aims to achieve, based on its strategic objectives, risk tolerance, and stakeholder expectations.

4. Governing Laws & Regulations

Guidance	Section
Australian Privacy Act 1988	• All
NSW Privacy and Personal Information Protection Act 1998	• Security Protection Principle (Clause 13, Section 11)
NSW health Records and Information Privacy Act 2002	• Section 11 - Security Safeguards
Essential 8	• All

5. Policy Statements

#	Policy Statement	Mapped Regulations/Standards
1.	COBLH will develop a process for the creation, review, and approval of information security policies.	NIST CSF: ID. GV-1 SOC2: CC5.3 ISO 27001: 5.2 ISO 27002: 5.1 PCI3: 12.1 PCI4: 12.1.2 HIPAA: §164.308(a)(1)(i)
2.	Dedicated policies will be developed for needed areas of information security.	NIST CSF: ID. GV-1, PR. IP-12 NIST 800-53: AC-1, AU-1, CA-1, IA-1, IR-1, MA-1, MP-1, PE-1, RA-1, SA-1, SC-1, SI-1, SR-1 SOC2: CC5.3, CC5.2 ISO 27002 5.1.1 PCI3: 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.9, 11.6 PCI4: 1.1.1, 2.1.1, 3.1.1, 4.1.1, 5.1.1, 6.1.1, 7.1.1, 8.1.1, 9.1.1, 10.1.1, 11.1.1, 12.1.1, 12.1.3 HIPAA: §164.308(a)(1)(i), §164.308(a)(3)(i), §164.308(a)(4)(i), §164.308(a)(6)(i), §164.310(a)(1), §164.310(b), §164.310(d)(1), §164.312(a)(1), §164.312(a)(1), §164.312(c)(1)
3.	Security policies will be distributed to all necessary employees and communicated effectively.	NIST CSF: ID. GV-1 NIST 800-53: AC-1, AU-1, CA-1, IA-1, IR-1, MA-1, MP-1, PE-1, RA-1, SA-1, SC-1, SI-1, SR-1 SOC2: CC2.2, CC5.3 ISO 27002 5.1.1 PCI4: 12.1.1 HIPAA: §164.316(b)(1)
4.	Security policy exceptions will be documented and approved by an executive and then logged in the Risk management system where appropriate.	NIST CSF: ID. GV-1 SOC2: CC5.3 ISO 27002 5.1
5.	Security policies will be enforced and implemented across the enterprise, with embedded violation handling protocols.	NIST CSF: ID. GV-1 NIST 800-53: PS-8 SOC2: CC1.5, CC5.3 ISO 27002 5.1, 5.4, 5.36, 6.4 HIPAA: §164.308(a)(1)(i), §164.308(a)(1)(ii)(C), §164.316(a)
6.	Security policies will be regularly reviewed, evaluated, and updated.	NIST CSF: ID. GV-1 NIST 800-53: AC-1, AU-1, CA-1, IA-1, IR-1, MA-1, MP-1, PE-1, RA-1, SA-1, SC-1, SI-1, SR-1 SOC2: CC5.3 ISO 27002 5.1 PCI3: 12.1.1 PCI4: 12.1.2 HIPAA: §164.308(a)(8), §164.316(b)(1) (i), §164.316(b)(2)(i), §164.316(b)(1)
	Information Security Program	
7.	A target state for information security will be defined and will reflect the expectations and requirements of key stakeholders.	NIST CSF: ID.BE-3 NIST 800-53: PL-2 ISO 27001: 4.2
8.	The scope of information security programs will be fully defined.	NIST CSF: ID.BE-4 NIST 800-53: PL-2 SOC2: CC5.1, CC5.2 ISO 27001: 4.3 PCI4: 12.5.2, 12.5.2.1, 12.5.3
9.	The target state for information security will reflect the security risks to the organization, including specific industry sector and geographic risks.	NIST CSF: ID.BE-1, ID.BE-2 NIST 800-53: PL-2 SOC2: CC3.1, CC3.4, CC5.1 ISO 27001: 4.1, 6.1.2 HIPAA: § 164.306 (b)(2), §164.308(a)(1)(ii)(A)
10.	The governance structure for information security will be defined.	NIST CSF: ID. GV-2, ID. GV-4 SOC2: CC1.3
11.	COBLH will develop an information security strategy	NIST CSF: ID.BE-3

	and roadmap for achieving the security target state.	NIST800-53: PL-1, PL-2, PL-10, PL-11 SOC2: CC5.1, CC5.2 ISO 27001: 4.4, 6.1.1, 6.1.3, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.1 HIPAA: §164.308(a)(1)(ii)(B)
12.	COBLH will ensure the information security program has adequate resources and support to meet its defined goals.	ISO 27001: 5.1
	Security Metrics	
13.	Metrics must be defined to measure the effectiveness of the security program.	NIST CSF: PR. IP-7, PR. IP-8 NIST 800-171: 3.12.3 NIST 800-53: CA-7 CMMC CA. L2-3.12.3 SOC2: CC2.1 ISO 27001: 9.1
14.	Ensure security metrics are communicated to relevant stakeholders.	NIST CSF: PR. IP-8 NIST 800-53: CA-7 SOC2: CC2.1 ISO 27001: 9.1, 9.3
15.	Metrics provided to senior management should be actionable and support decision making.	SOC2: CC2.1 ISO 27001: 9.1
16.	Develop a process to continuously improve the security program based on collected metrics.	NIST CSF: PR. IP-7 NIST 800-171: 3.12.3 NIST 800-53: CA-7 CMMC CA. L2-3.12.3 SOC2: CC2.1 ISO 27001: 9.1, 10.1

1. Development, Review, and Approval of Information Security Policies: COBLH has a robust process for the creation, review, and approval of information security policies. This process involves the development of policies based on industry standards by the IT Director and the Cybersecurity Team. These policies are then reviewed by the Health Executive Committee (HEC) for comments and discussions. The final step in this process is the approval of the policies by the Audit and Risk Committee (ARC) and then by the Board.

2 & 3. Dedicated Policies and Distribution: COBLH develops dedicated policies for each area of information security. These policies are then distributed to all relevant employees. To ensure effective communication of these policies, COBLH uses various methods, such as email notifications, policy briefings, or training sessions, depending on the nature and importance of the policy.

4. Policy Exceptions: Any exceptions to the security policies are carefully documented and approved. This process involves identifying the need for an exception, evaluating the associated risks, and getting approval from the appropriate authority. The approved exceptions are then documented, along with their justification and the measures taken to manage the associated risks.

5. Policy Enforcement and Violation Handling: COBLH is committed to enforcing its security policies across the enterprise. This includes implementing the policies in all relevant systems and processes, educating employees about their responsibilities, and monitoring compliance. Any violations of the policies are handled in accordance with the established protocols, which may include investigations, corrective actions, and disciplinary measures, as appropriate.

6. Regular Review and Update of Policies: COBLH ensures that its security policies remain effective and up to date by conducting regular reviews and updates. The IT Director and the Cybersecurity Team are responsible for this process, which involves evaluating the policies in light of any changes in the organisation's systems, operations, or risk environment, as well as

6. Target State

The target state for information security in COBLH is as follows;

Compliance with Regulatory Requirements: Achieve and maintain compliance with relevant laws and regulations, such as the Privacy Act 1988, the Health Records and Information Privacy Act 2002 (NSW), and the Essential 8 where applicable.

Enhanced Security of Patient Data: Maintain and enhance strong access controls, encryption, and data loss prevention measures to protect sensitive patient information from unauthorized access, disclosure, or alteration.

Robust Identity and Access Management: maintain and enhance a comprehensive identity and access management framework to ensure that only authorised personnel have access to critical systems and data, and that access is granted based on the principle of least privilege.

Security Awareness and Training: Maintain and enhance a continuous security awareness and training program to educate staff on their responsibilities related to information security, including the identification and reporting of potential security incidents.

Advanced Threat Detection and Response: Maintain and enhance advanced security monitoring and incident response capabilities, including intrusion detection and prevention systems, endpoint protection, and a Security Information and Event Management (SIEM) system, to quickly detect and respond to potential cyber threats.

Business Continuity and Disaster Recovery: Maintain and enhance a comprehensive business continuity and disaster recovery plan to ensure the hospital can continue to provide critical services and maintain the availability of essential data in the event of a security incident or other disruptive event.

Third-Party Risk Management: Maintain and enhance a rigorous third-party risk management process to evaluate and manage the security risks associated with vendors, suppliers, and other external entities that have access to the hospital's systems or data.

Continuous Improvement: Maintain a culture of continuous improvement, with regular reviews of the hospital's information security posture, processes, and technologies to identify areas for enhancement and ensure alignment with industry best practices and evolving threat landscapes.

7. Governance Structure

The governance structure for information security at COBLH is organised as follows;

Board of Directors: The board is ultimately responsible for overseeing the information security program at COBLH, including approving policies and budgets, and understanding the risks associated with information security.

Audit and Risk Committee (ARC): The ARC assists the board in fulfilling its oversight responsibilities. It reviews and recommends approvals information security policies before they are sent to the board. It also reviews reports on information security risks and the effectiveness of the security program.

Health Executive Committee (HEC): The HEC reviews, comments on, and discusses information security policies before they are sent to the ARC. This ensures that the policies are aligned with the organization's healthcare mission and objectives.

IT Director: The IT Director is responsible for developing and managing the information security program. This includes creating and regularly reviewing security policies, managing the security team, coordinating risk assessments, and implementing security controls.

Cybersecurity Team: The Cybersecurity Team is all the IT team plus a dedicated Cybersecurity Analyst and assists the IT Director in the management of the security program. This includes identifying and analysing security threats and vulnerabilities, monitoring compliance with security policies, and investigating security incidents.

All Employees: All employees, VMOs and contractors are responsible for complying with the organisation's information security policies. They also have a role to play in identifying and reporting potential security issues.

8. Scope of Information Security Program

Defining the scope of an information security program is essential to understand what assets, risks, and processes are covered and governed. Below is how the scope of the information security program at COBLH is defined:

Assets - covers all information assets owned or used by COBLH, whether they are physical or digital. This includes servers, computers, mobile devices, network equipment, software applications, and databases. It also includes data, such as patient records, financial information, employee data, intellectual property, and other sensitive or proprietary information.

Processes - applies to all business processes that involve the use, storage, transmission, or disposal of information assets. This includes clinical processes, administrative processes, financial processes, IT processes, and any other processes that could affect the confidentiality, integrity, or availability of information assets.

Locations - applies to all locations where COBLH operates or where its information assets may be located. This includes the COBLH main hospital. It also includes any offsite locations where data may be stored, processed, or transmitted, such as cloud service providers.

People: - all people who have access to COBLH's information assets. This includes all employees, contractors, vendors, volunteers, and any other individuals who may use, process, store, or interact with any data belonging to the organisation's or within the organisation.

Threats - addresses all types of information security threats, whether they are internal or external, deliberate or accidental. This includes threats like malware, ransomware, hacking, insider threats, human error, physical theft, social engineering, natural disasters, and any other threats that could harm the organisation's information assets.

Legal and Regulatory Requirements - takes into account all legal and regulatory requirements related to information security that COBLH must comply with. This includes laws and regulations related to data protection, privacy, health information, financial information, and any other

relevant areas.

9. Information Security Strategy

COBLH has performed an extensive analysis of our current information security posture, identifying several opportunities for improvement. In response to these findings, we have developed a comprehensive strategy that outlines our desired target state for information security, which incorporates several key principles.

This future state aligns with and supports our commitment to adhering to all regulatory requirements, ensuring the secure management of data, and implementing a robust identity and access management system. Our strategy further prioritises continuous employee training to ensure that all staff members are informed about the latest best practices and potential threats.

Advanced threat detection capabilities have been integrated into our security measures to swiftly identify and address potential threats, thereby reducing potential damage. As part of our risk mitigation efforts, business continuity planning will be a cornerstone of our strategy, ensuring minimal operational disruption in the face of unforeseen events.

Recognising the potential risks presented by third-party associations, our security strategy also incorporates a strong third-party risk management approach. To ensure the ongoing effectiveness and responsiveness of our security measures, we will also foster a culture of continuous improvement that encourages adaptation and innovation in our security practices.

In terms of frameworks, COBLH has adopted the Essential 8 model to help structure our systems and processes to measurable outcomes. At all times COBLH will aim to achieve the highest possible maturity level within the essential 8 model. However, we recognise for some areas this will not be possible and have noted them when reporting to the board on our essential 8 progress. Alongside this, we will also align our strategy with the ISO 27001 standard, an internationally recognised standard for Information Security Management Systems (ISMS). This dual-framework approach will provide a structured methodology to guide us in improving our security measures over the coming years. Performance metrics

1. **Number of Incidents:** Track the number of security incidents reported and resolved. A decrease in the number over time may suggest an improvement in security.
2. **Time to Detect:** Measure the average time it takes to detect a security incident from the time it occurs. A shorter detection time usually means your systems are effectively monitoring and alerting on potential security issues.
3. **Time to Respond:** Measure the average time it takes to respond to a security incident once it has been detected. This includes the time taken to contain, eradicate and recover from the incident. A shorter response time usually indicates a more efficient incident response process.
4. **Patch Management:** Track the average time it takes to apply security patches after they are released. A shorter patch time may indicate a more efficient patch management process.
5. **Training Participation Rate:** Measure the percentage of employees who have completed mandatory security awareness training. A high participation rate is crucial for reducing the risk of security incidents caused by human error.
6. **Phishing Test Failure Rate:** If you conduct simulated phishing exercises, track the percentage of employees who click on a mock phishing email. A decrease in this rate over time may suggest that your awareness training is effective.
7. **Compliance Metrics:** Track your compliance with relevant regulatory standards. This could include the percentage of systems that meet specific security requirements, or the

number of non-compliance issues identified during audits.

These metrics can help COBLH track its progress toward achieving the target state for information security and provide valuable insights for decision-making and continuous improvement.

COBLH is committed to maintaining transparency and continuous improvement in its security program. Accordingly, we will regularly communicate key security metrics to relevant stakeholders, including IT staff, management, and the board of directors. These metrics, which include incident numbers, detection and response times, patch management efficiency, training participation, phishing test failure rates, and compliance levels, will be presented in a clear, concise manner that supports informed decision-making.

Furthermore, these metrics will serve as a foundation for the continuous improvement of our security program. By regularly analysing these metrics, we can identify trends, detect potential issues early, and assess the effectiveness of our current strategies. This information will guide our decision-making process and help us adjust our strategies and protocols as needed to enhance the overall security posture of COBLH.

10. Defining an Incident

An incident refers to an event or series of events that could lead to a loss or disruption of COBLH operations, services, or functions. An incident could potentially breach security and cause a system's confidentiality, integrity, or availability to be compromised.

Levels of an incident:

Critical: These Security Incidents represent significant losses of company data, a 'notifiable' data breach, and/or pose a possible threat to data integrity.
High: These Security Incidents affect the availability of information; however, data integrity is not affected.
Moderate: A moderate cybersecurity breach involves unauthorised access or compromise of non-critical systems, which may have some negative impact on the organisation.
Minor: localised to a particular workstation, such as virus activity causing no threat to critical company data.
Minimal: A problem that does not affect the functionality of the user, system or application

11. Measuring Performance Metrics

COBLH uses the below tools to keep track of our performance metrics:

Incidents, Time to Detect, and Time to Respond: COBLH is using CrowdStrike. This will help us log all the incidents, find out how long it takes to spot them, and how quickly we respond.

Patch Management: For managing and recording how quickly we apply security patches, COBLH is using N-Central. N-Central provides indepth reports on each device and its patch status.

Training Participation: COBLH is monitoring security awareness training through HETI. Reports will be run to see which employees are required to complete the security modules.

Phishing Tests: After we've run our fake phishing tests to see who might fall for these types of scams, we'll make a manual record of the results.

We will take the data gathered from CrowdStrike, N-able, HETI, and our manual phishing tests and combine it all into a comprehensive report. This report will allow COBLH to compare our current performance to our past results. This way, we can see clearly where we're improving, and where we might need to put in more work.

COBLH is committed to running these performance metrics every year. So, annually, we'll have a clear, detailed picture of our security situation and how it's evolving. We'll use this information to make sure COBLH is as secure as possible and continues to improve.

12. Noncompliance

Violations of this policy will be treated like other allegations of wrongdoing at COBLH. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable COBLH policies.
2. Termination of employment.
3. Legal action according to applicable laws and contractual agreements.