UNIVERSITY of TASMANIA

KIT515 – Cybersecurity Policies and Practices

Group Assignment (Group Number : 2)

Company name: TanuCare Pty Ltd

Member Name	Student ID
Parth Patel	684138
Ravi Savani	685167
Malay Prajapati	683905
Md Khalil	706786

Table of Contents

1.1: Executive Summary

TanuCare Pty Ltd is a health-tech robotics enterprise based in Tasmania, offering intelligent robotic assistants, remote care platforms, and health service automation. With the growing reliance on connected medical technologies, safeguarding sensitive health data and ensuring service continuity is a critical requirement for the organisation. This document outlines a comprehensive cybersecurity strategy designed to protect TanuCare's physical infrastructure, digital systems, customer data, and overall operational integrity.

The primary objective of this report is to present a cybersecurity framework that aligns with TanuCare's mission to deliver compassionate, technology-driven care solutions while addressing the pressing cybersecurity risks present in the health-tech sector. As TanuCare expands its services to aged care facilities, families, and clinics, its threat profile intensifies, especially in areas involving personal health information, cloud infrastructure, robotic firmware, and remote monitoring tools.

Through qualitative and quantitative risk assessments, critical assets were identified across four key domains: hardware, software, data, and business operations. Each asset was analysed for potential threats, vulnerabilities, and associated risks. The analysis revealed key concerns such as ransomware, IoT bot compromise, insider threats, and data breaches targeting the appointment and monitoring platform. These findings informed the development of risk mitigation strategies and targeted security policies.

The report proposes a multi-layered cybersecurity model that incorporates administrative, technical, and physical controls. High-level policies address secure configuration management, access control, data encryption, patching, employee training, and incident reporting protocols. These policies serve as a foundation for the detailed recommendations included in Section 2 of the report, where each asset category is addressed in depth.

Our risk analysis covered five asset domains Hardware, Software, Data, Business Operations and Acceptable Use identifying two critical threats (DA-01: Data Breach and HW-03: IoT Compromise) along with multiple high and medium level risks. Section 1.4 then presents a six phase Incident Response Plan with clearly defined roles, escalation paths and Notifiable Data Breach (NDB) reporting triggers. In Section 1.5, we map six key security issues to ten overarching policies (P01–P10) for governance and enforcement. Sections 2.1 through 2.5 provide in-depth, domain-specific controls from endpoint hardening and secure coding to vendor management and staff awareness supported by full risk tables, heat-maps and flowcharts in the appendices.

An incident response plan has been developed to guide TanuCare’s approach to detection, containment, eradication, and recovery in the event of a security incident. This plan includes clear roles and escalation pathways for all internal stakeholders and aligns with Australia’s Notifiable Data Breach (NDB) scheme.

This report also recognises the ethical responsibilities inherent in healthcare robotics. TanuCare’s policies are built on the principles of privacy, transparency, and accountability. Security awareness and training programs are central to the organisational culture to ensure both staff and clients are equipped to interact safely with emerging technologies.

In conclusion, this cybersecurity policy framework is designed not only to secure TanuCare’s systems and services but also to uphold its core values of trust, empathy, and innovation. By proactively addressing cybersecurity challenges, TanuCare strengthens its reputation as a safe and reliable care technology provider in Tasmania and beyond.

1.2: Introduction – TanuCare Case Study

TanuCare Pty Ltd is a medium-sized health-tech enterprise headquartered in Hobart, Tasmania, with a growing reputation for delivering compassionate and technology-driven solutions in the aged care, childcare, and health service sectors. The organisation specializes in the design and deployment of intelligent robotic assistants, secure cloud-based platforms, and remote health monitoring systems. As Tasmania faces challenges such as long appointment waiting times, aged care staff shortages, and service access limitations in rural areas, TanuCare has positioned itself as a critical player in addressing these regional health and service gaps.

Established in response to rising demand for ethical, efficient, and scalable care solutions, TanuCare currently employs 130 staff members across three locations: Hobart (headquarters and Security Operations Centre), Launceston (robotics engineering and software development), and Devonport (customer care and NDIS onboarding). The company operates with an estimated annual revenue of AUD 14.8 million and serves both government and private-sector clients, including aged care facilities, general practitioners, disability support providers, and families seeking home-based care automation.

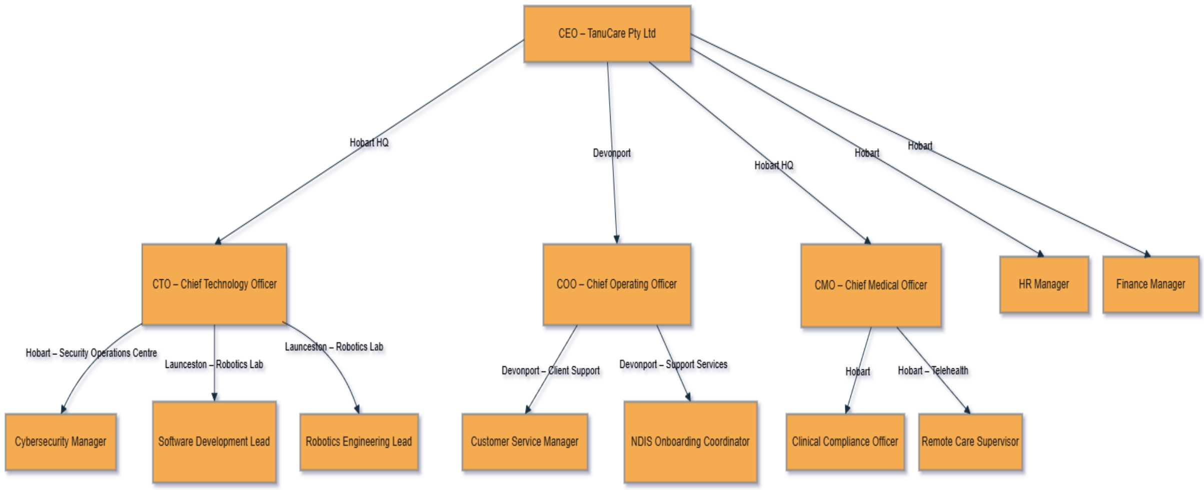

CEO – TanuCare Pty Ltd
Hobart HQ
Devonport
Hobart HQ
Hobart
Hobart
CTO – Chief Technology Officer
COO – Chief Operating Officer
CMO – Chief Medical Officer
HR Manager
Finance Manager
Hobart – Security Operations Centre
Launceston – Robotics Lab
Launceston – Robotics Lab
Devonport – Client Support
Devonport – Support Services
Hobart
Hobart – Telehealth
Cybersecurity Manager
Software Development Lead
Robotics Engineering Lead
Customer Service Manager
NDIS Onboarding Coordinator
Clinical Compliance Officer
Remote Care Supervisor

Figure 1: Organisational Structure of TanuCare Pty Ltd

TanuCare's product offerings include CareBots—AI-powered robotic companions that assist with daily routines such as medication reminders, mobility support, and emergency response. These bots are complemented by the TanuCare mobile app, which enables secure appointment bookings, video consultations, and remote vitals monitoring. The company's cloud infrastructure integrates seamlessly with Medicare and the National Disability Insurance Scheme (NDIS), providing automated reporting, invoicing, and care documentation capabilities.

To support its service delivery, TanuCare maintains a hybrid ICT environment combining AWS-hosted services with on-premises R&D servers and secure APIs for bot-to-cloud communication. The organisation employs encrypted MQTT protocols for IoT device communication, endpoint protection tools for mobile workforce devices, and continuous integration/deployment (CI/CD) pipelines for rapid software updates.

In alignment with Tasmania's commitment to sustainability and digital transformation, TanuCare ensures its operations are powered by renewable energy sources. Its robotics are built with recyclable components and follow ethical AI design principles. Moreover, the company actively contributes to local workforce development through partnerships with the University of Tasmania (UTAS) and TAFE institutions, offering internships and upskilling programs in health informatics and robotics.

Given the sensitive nature of TanuCare's operations—particularly the handling of patient health data, cloud services, and AI-based robotic devices—the company is exposed to a broad range of cybersecurity threats. These include risks related to data breaches, ransomware, compromised IoT firmware, phishing attacks, and insider misuse. A well-defined and proactive cybersecurity strategy is therefore essential to protect TanuCare's assets, maintain public trust, and ensure compliance with relevant standards such as the Notifiable Data Breach (NDB) scheme, the Privacy Act 1988 (Cth), and the Australian Cyber Security Centre's Essential Eight framework.

This report builds upon the context described in this case study and proceeds to assess the organisation's critical assets, associated risks, and cybersecurity controls. The goal is to design a comprehensive and context-sensitive policy framework that enhances

TanuCare's overall cyber resilience while enabling continued innovation in healthcare robotics and remote care delivery.

1.3: Risk Analysis

Effective cybersecurity begins with a thorough understanding of the organisation's assets, their associated threats and vulnerabilities, and the likely consequences of exploitation. TanuCare, as a health-tech robotics enterprise, operates in a threat landscape that includes not only general cyber risks but also those uniquely tied to IoT, artificial intelligence, health data, and national digital health infrastructure. This section presents the qualitative and quantitative risk analysis conducted for TanuCare, forming the foundation for its cybersecurity policies and incident response planning.

---

1. Asset Identification

TanuCare's critical assets are categorized into four domains:

1.1 Hardware Assets

- HQ servers (HW-01)
- Robotics lab machines (HW-02)
- Customer-deployed CareBots (HW-03)
- Mobile devices for field staff (HW-04)
- CCTV and access control systems (HW-05)

1.2 Software Assets

- TanuCare App and backend APIs (SW-01)
- Firmware for robots (SW-02)
- CI/CD and DevOps infrastructure (SW-03)
- Third-party integrated systems (e.g., NDIS, Medicare portals) (SW-04)
- Office productivity tools (SW-05)

1.3 Data Assets

- Client health data and NDIS records (DA-01)
- Video/audio data from CareBots (DA-02)
- Internal logs and audit trails (DA-03)
- Source code repositories (DA-04)
- HR and financial records (DA-05)

1.4 Business Assets

- Brand reputation and trust (BA-01)
- Regulatory compliance status (BA-02)

- Availability of care services (BA-03)
- Intellectual property (BA-04)
- Third-party partner relationships (BA-05)

Each asset has been assigned a **weighted value** based on its business impact. Assets such as client health data (DA-01), deployed robots (HW-03), and the TanuCare App (SW-01) received the highest weighting due to their direct connection to service delivery, legal obligations, and public trust.

---

2. Threats, Vulnerabilities, and Controls

The risk assessment identified key threats applicable to TanuCare:

Threat	Description	Affected Assets
Ransomware	Encrypts vital data and halts operations	SW-01, DA-01, BA-03
IoT Bot Compromise	Remote control of CareBots via firmware flaws	HW-03, SW-02
Data Breach	Unauthorized access to sensitive health data	DA-01, DA-02, SW-04
Insider Threat	Staff misuse of privileged access	DA-04, HW-04, BA-04
Phishing/Social Engineering	Credential theft through fake emails or calls	BA-05, SW-05
Patch Failure	Exploitable systems due to delayed updates	HW-01, SW-03

Existing controls include multi-factor authentication, encryption (AES-256) for all health data, endpoint detection and response (EDR) for mobile devices, and regular access reviews. However, gaps were identified in firmware update processes, patch automation, and monitoring of deployed CareBots in customer homes.

3. Qualitative Risk Assessment

A **likelihood vs. impact matrix** was used to assess each threat to each asset. An example:

Asset Code	Threat	Likelihood	Impact	Risk Level
DA-01	Data Breach	High	High	**Critical**
HW-03	IoT Compromise	Medium	High	**High**
SW-02	Firmware Exploit	Medium	Medium	**Medium**
BA-03	Ransomware Outage	Low	High	**Medium**

Asset Code	Threat	Likelihood	Impact	Risk Level
DA-04	Insider Leak	Medium	High	**High**
SW-03	Patch Failure	High	Medium	**High**

This analysis shows that data breaches, insider threats, and compromised CareBots are the most urgent risks. Ransomware and social engineering attacks, though slightly lower in likelihood, pose serious business continuity concerns and are treated with similar caution.

4. Quantitative Risk Assessment

A numerical scoring model was used where:

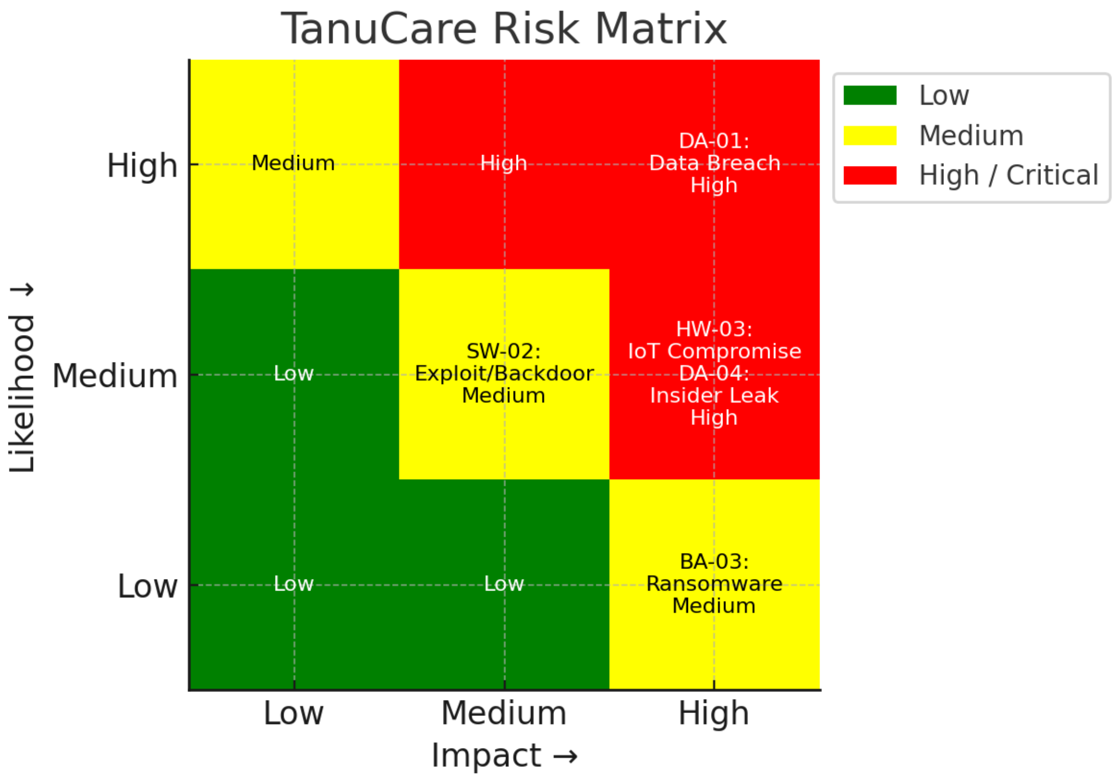
- **Likelihood**: 1 (Low), 2 (Medium), 3 (High)
- **Impact**: 1 (Minor), 2 (Major), 3 (Severe)
- **Risk Score = Likelihood × Impact**

Sample results:

Asset	Threat	Likelihood	Impact	Score	Risk Level
DA-01	Data Breach	3	3	9	**Critical**
HW-03	IoT Hijack	2	3	6	High
SW-02	Firmware Flaw	2	2	4	Medium
BA-01	Reputation Damage	1	3	3	Medium
DA-03	Log Tampering	1	2	2	Low

Any score of **6 or above** is considered **high priority** for immediate mitigation.

Risk Matrix (Heat Map):



5. Risk Mitigation Planning

Based on the results, mitigation strategies include:

- **P01**: Mandatory firmware signing and OTA update verification for all CareBots
- **P02**: Role-based access control and automated logging for all backend systems
- **P03**: Bi-weekly security patch cycles and real-time monitoring for anomalies
- **P04**: End-user security awareness training, especially for phishing risks
- **P05**: Backup and recovery testing every 30 days to ensure ransomware resilience
- **P06**: Encryption of data at rest and in transit using industry standards

Each policy is linked to one or more high-risk assets and threats and will be detailed in Section 1.5.

---

6. Emerging Threat Considerations

TanuCare's use of robotics and AI introduces additional risks such as:

- **Adversarial machine learning**, where attackers poison training data to affect bot behavior
- **Voice or image spoofing**, which could manipulate bots' sensors or cause false responses
- **Legal grey areas** around responsibility for bot actions (ethical AI concerns)

As the business grows, policies must be adaptable to future threats involving AI, biometric interfaces, and smart home integration.

Conclusion

This risk analysis confirms that TanuCare's core risks relate to data protection, IoT integrity, insider threats, and service continuity. By identifying asset-specific threats and prioritizing mitigation based on business impact and likelihood, the organisation is positioned to design a robust cybersecurity policy framework. This assessment directly informs the incident response strategy and policy recommendations detailed in subsequent sections of the report.

1.4: Incident Response Plan

TanuCare's reliance on cloud-connected robots, sensitive health data, and distributed IT infrastructure makes it a prime target for a range of cyber incidents, including ransomware, data breaches, firmware tampering, and insider threats. As a provider of health-tech services, TanuCare is legally and ethically obligated to respond quickly and transparently to any event that may compromise the confidentiality, integrity, or availability of its systems or client data.

This incident response plan (IRP) outlines the structured approach TanuCare will follow when responding to cybersecurity incidents. The plan is designed to minimise damage, reduce recovery time and costs, and ensure compliance with relevant legal requirements, including the **Privacy Act 1988 (Cth)** and the **Notifiable Data Breaches (NDB) scheme**.

---

1. Incident Response Objectives

The primary goals of this incident response plan are to:

- Detect and confirm security incidents quickly
- Contain and mitigate the spread or impact of an incident
- Eradicate the root cause and restore normal operations
- Document lessons learned and improve policies
- Fulfil legal obligations for breach notification

---

2. Roles and Responsibilities

Role	Responsibility
Incident Response Manager (CTO)	Leads and coordinates response; activates IRP
Security Analyst	Investigates logs, isolates affected systems
IT Operations Lead	Restores backups, applies patches, monitors recovery
Legal/Compliance Officer	Advises on NDB reporting and stakeholder communications
Communications Officer	Coordinates internal and external messaging
HR Representative	Involved if the incident involves an insider or policy breach

Each team member has pre-assigned roles and contact escalation chains, documented internally and tested quarterly.

---

3. Incident Response Phases

TanuCare follows the industry-standard six-phase incident response lifecycle:

1. Preparation

- Maintain updated policies, backups, and contact lists
- Regular incident response simulations and security awareness training

2. Identification

- Detect anomalies using EDR, firewall logs, user reports, or CareBot behaviour
- Validate incidents against predefined threat indicators

3. Containment

- Short-term: Disconnect affected CareBots or servers from networks
- Long-term: Quarantine systems, revoke access, begin forensic collection

4. Eradication

- Remove malware, patch vulnerabilities, reset credentials
- Check for persistence or lateral movement in systems

5. Recovery

- Restore data from verified backups
- Monitor systems for signs of reinfection
- Gradually reintroduce systems to the network under close observation

6. Lessons Learned

- Conduct a post-incident review within 5 business days
- Document the timeline, root cause, resolution, and areas for improvement
- Update incident response documentation and training if necessary

---

4. Legal & Regulatory Compliance

If personal or health information is breached, the Legal Officer will determine whether the incident qualifies under the **Notifiable Data Breaches (NDB) scheme**. If so:

- The **Office of the Australian Information Commissioner (OAIC)** must be notified within 30 days
- Affected individuals must be informed directly
- A public breach notification (if applicable) must be posted on the company website

TanuCare retains legal and incident logs for a minimum of 5 years.

---

5. Tools and Communication Channels

- **Communication Tools**: Microsoft Teams, Secure Email, Emergency Hotline
- **Monitoring Tools**: SIEM, EDR, real-time alert dashboards
- **Documentation**: All incidents logged in the company's secure IRP database (based on MITRE ATT&CK tagging)

Conclusion

TanuCare's incident response plan is designed to ensure a fast, coordinated, and compliant reaction to cybersecurity events. It establishes clear responsibilities, communication pathways, and legal processes to preserve trust and reduce operational disruption. This plan will be reviewed bi-annually or immediately after any major incident to maintain relevance in an evolving threat landscape.

1.5: Security Issues and High-Level Policies

The implementation of effective cybersecurity policies at TanuCare is essential to mitigate the risks identified in the risk analysis and support rapid, coordinated incident response. This section outlines the key security issues currently facing the organisation and presents high-level policies designed to address them. These policies are cross-referenced with the asset codes and threat scenarios from the risk register and are designed to align with national standards, including the Australian Cyber Security Centre's Essential Eight framework and the Notifiable Data Breaches (NDB) scheme.

---

1. Key Security Issues

1.1 Exposure of Sensitive Health Data (DA-01, DA-02)

TanuCare stores and processes sensitive health data and NDIS information, including video/audio from CareBots. A breach of this data would result in severe legal, financial, and reputational consequences under the NDB scheme.

1.2 Compromise of IoT CareBots (HW-03, SW-02)

The customer-deployed robots operate in private environments and are remotely connected to TanuCare's cloud systems. Their firmware could be exploited if not properly secured and monitored.

1.3 Insider Threats and Privileged Misuse (DA-04, HW-04)

With staff working across multiple locations and remotely, there is a heightened risk of internal misuse or accidental leakage of sensitive assets such as source code, logs, and HR data.

1.4 Ransomware and Service Availability Risks (BA-03, SW-01)

Interruptions to TanuCare's appointment booking, remote monitoring, or CareBot communication services could directly impact vulnerable clients and the company's business operations.

1.5 Patch and Firmware Management Gaps (SW-02, HW-01)

Delayed or incomplete updates to software and robot firmware may leave systems vulnerable to known exploits, especially when deployed in uncontrolled environments.

1.6 Weak User Security Awareness (BA-05, SW-05)

Staff and client-side users may fall victim to phishing, credential reuse, or accidental data exposure, particularly due to a lack of formal training programs.

---

2. High-Level Security Policies

Below is a set of ten high-level policies, each aligned to the risk profile and designed to be implemented across relevant TanuCare departments and systems.

P01 – Data Encryption Policy

All sensitive data (DA-01, DA-02) must be encrypted at rest and in transit using AES-256 or industry-standard protocols.

Applies to: Cloud storage, CareBot video/audio streams, health records

Linked Assets: DA-01, DA-02, SW-01

P02 – Firmware Update and Integrity Policy

All robot firmware must be cryptographically signed and updated through Over-The-Air (OTA) secure channels. Devices must reject unauthenticated updates.

Applies to: CareBots, lab devices

Linked Assets: HW-03, SW-02

P03 – Access Control and Privilege Management Policy

User access must follow the principle of least privilege. Admin access must be role-based, with activity logging and regular access reviews every quarter.

Applies to: DevOps platforms, NDIS portals, internal apps

Linked Assets: SW-03, DA-04, HW-04

P04 – Ransomware Mitigation and Recovery Policy

Daily backups must be taken and stored in separate networks. Ransomware simulation and restore testing must be performed monthly to ensure data recovery capability.

Applies to: TanuCare App, client data, business records

Linked Assets: SW-01, BA-03, DA-01

P05 – Patch and Update Compliance Policy

All software and hardware systems must undergo security patching within 7 days of public vulnerability disclosure. Firmware updates must be logged and verified.

Applies to: Internal servers, robots, productivity tools

Linked Assets: HW-01, SW-02, SW-05

P06 – Security Awareness and Training Policy

All employees must complete mandatory cybersecurity training every 6 months, including modules on phishing, data handling, and password hygiene.

Applies to: All staff and contracted developers

Linked Assets: BA-05, SW-05

P07 – Incident Reporting and Escalation Policy

All cybersecurity incidents must be reported to the Incident Response Manager within 30 minutes of discovery. Escalation flow must follow the incident response protocol.

Applies to: All departments and systems

Linked Assets: All

P08 – Logging and Monitoring Policy

Critical systems must maintain logs of all access, changes, and transactions for a minimum of 12 months. Logs must be reviewed weekly and stored securely.

Applies to: Servers, CareBots, software platforms

Linked Assets: DA-03, HW-01, SW-01

P09 – Third-Party Integration Policy

Third-party services (NDIS, Medicare, APIs) must be reviewed for compliance before integration. Contracts must include cybersecurity clauses and breach notification timelines.

Applies to: Partner services and integrations

Linked Assets: SW-04, BA-02

P10 – Acceptable Use and Device Security Policy

Staff must use only company-approved devices and follow acceptable use guidelines. External devices must be scanned before connection. Personal use is prohibited on production systems.

Applies to: All workstations, mobile devices

Linked Assets: HW-04, BA-04

---

3. Policy Governance and Enforcement

Each policy will be managed by the Cybersecurity Manager and reviewed annually during internal audits. Violations of these policies will result in disciplinary action or access restrictions, depending on severity. Policies will be shared through the company intranet, and compliance will be tracked via the LMS and asset management platforms.

All policies align with:

- ACSC Essential Eight
- ISO/IEC 27001:2022
- Privacy Act 1988 (Cth)
- OAIC Notifiable Data Breach scheme

Conclusion

TanuCare's security policies directly address its key operational risks and lay the foundation for secure robotics and health-tech service delivery. By implementing these high-level controls and ensuring ongoing compliance, TanuCare reinforces its commitment to client safety, legal responsibility, and innovation. Each policy is further operationalised in Section 2 of this report, where asset-specific recommendations and procedures are presented.

2.1: Security for Hardware Assets (Made by Parth Patel)

1. Overview

TanuCare's hardware infrastructure includes a combination of in-house and deployed systems, each critical to service delivery. The most significant components include CareBots used in patient homes and aged care facilities, backend servers hosted at Hobart HQ, robotics lab hardware in Launceston, mobile devices used by field staff, and physical security equipment such as CCTV and access control panels. These assets play a direct role in providing care and monitoring, enabling cloud connectivity, and ensuring data acquisition and real-time decision-making.

Given their pivotal role and their exposure to both physical and digital threats, securing hardware assets is essential for ensuring data confidentiality, maintaining system integrity, and delivering uninterrupted health services. This section proposes security strategies based on the risks identified in Section 1.3 and the policy framework defined in Section 1.5.

2. Hardware Asset Inventory

Asset Code	Description	Location	Importance
HW-01	Backend Servers (Hobart HQ)	Data storage, APIs, backups	High
HW-02	Robotics Lab Devices (Launceston)	Firmware testing and R&D	High
HW-03	Deployed CareBots	Client homes, aged care	Critical
HW-04	Mobile Devices (Field Staff)	Remote support, diagnostics	High
HW-05	CCTV & Access Systems	Physical security	Medium

3. Threat Landscape

3.1 Physical Theft and Tampering

Devices in public or semi-controlled environments (CareBots, mobile devices) are at risk of theft or tampering. This is particularly critical for CareBots located in private homes.

3.2 Firmware Exploitation

Unpatched or unsigned firmware on CareBots can be modified, allowing attackers to hijack devices or leak sensitive data (HW-03).

3.3 Unauthorized Access

Loss or misuse of staff mobile devices (HW-04) can result in unauthorized access to cloud systems, especially if MFA is not enforced or devices are not encrypted.

3.4 Insider Threat

Staff with physical access to backend servers or robotics lab equipment may misuse administrative privileges or tamper with system configurations (HW-01, HW-02).

3.5 Surveillance System Exploits

CCTV and access control systems are vulnerable to firmware flaws or misconfigurations that could expose entry points or camera feeds (HW-05).

4. Security Goals for Hardware Assets

- Ensure physical and logical integrity of all critical hardware
- Prevent unauthorized access, tampering, and data extraction
- Secure firmware update mechanisms for deployed robots
- Maintain asset traceability and enforce chain-of-custody procedures
- Enforce compliance with Policy P02 (Firmware Integrity), P03 (Access Control), P05 (Patch Management), and P10 (Acceptable Use Policy)

5. Proposed Security Measures

5.1 Device Hardening and Physical Protection

- All servers (HW-01) and lab devices (HW-02) will be placed in locked server rooms with CCTV monitoring.
- CareBots (HW-03) will include tamper-evident seals and internal alerts triggered upon unauthorized access attempts.
- Mobile devices (HW-04) will use remote wipe, location tracking, and full-disk encryption.

5.2 Firmware Security (Policy Reference: P02, P05)

- All firmware deployed to CareBots must be signed using SHA-256 or higher cryptographic hashes.
- OTA firmware updates must pass verification checks before execution.
- Rollback protection will be enforced to prevent downgrading firmware to vulnerable versions.

5.3 Endpoint Access Control (Policy Reference: P03, P10)

- Device access must be restricted to authorised personnel only.
- All mobile devices must enforce MDM policies including mandatory PINs, biometric unlock, and automatic lockout after 5 failed attempts.

- Field support apps must include time-based token authentication linked to employee IDs.

5.4 Surveillance and Entry System Hardening (Policy Reference: P08)

- CCTV firmware must be updated monthly.
- Logs from access control panels will be centralised and reviewed weekly.
- Video feeds will be encrypted in transit and stored in segregated storage with access logs.

5.5 Inventory and Tracking

- Asset tags and serial numbers will be digitally logged in the central asset register.
- Chain-of-custody documentation will be required for any movement or reassignment of CareBots.
- Lost or stolen devices must be reported within 24 hours per Policy P07.

5.6 Lifecycle & Patch Management

- To ensure ongoing integrity of all hardware assets, TanuCare will establish a formal configuration baseline and patch management process. Every CareBot, edge device and server chassis must adhere to an approved security configuration standard, reviewed on a quarterly cadence. Critical firmware and OS updates will be tested in a staging environment and deployed to production within 14 days of vendor release. Decommissioned hardware undergoes secure data wipe and certified e-waste recycling to prevent data remanence.

5.7 Supply-Chain Security

- All hardware vendors must pass an ISO/IEC 27001–aligned security vetting before onboarding. Existing suppliers will be re-evaluated annually, with any findings tracked in the Vendor Risk Register (Policy P09).

5.8 Environmental & Power Controls

- All server rooms, robotics labs and field-deployed CareBot stations will be instrumented with continuous temperature, humidity and power-quality sensors. Threshold triggers (e.g. >30 °C or voltage <210 VAC) will automatically generate high-priority alerts to the NOC.
- Uninterruptible Power Supplies (UPS) with battery-backed redundancy will support key hardware for a minimum of 15 minutes during outages a secondary generator system will engage automatically for extended power failures.
- Clean-room standards (ISO 14644-1 Class 8) apply to lab environments; HVAC filters and airflow patterns are reviewed quarterly to prevent dust, moisture or particle ingress that could degrade hardware reliability.

5.9 Penetration Testing & Red-Team Exercises

- An external red-team will perform annual physical penetration tests on both data-centre and field hardware (CareBots, access panels), attempting lock-picking, tamper-shield bypass, and side-channel analysis on firmware.
- Simultaneously, network pentests will run against backend servers and device-management platforms to identify protocol exploits or misconfigured services. All findings must be remediated within 30 days.
- A combined "hybrid war-gaming" drill—mixing physical breach with cyber intrusion—is scheduled every two years to validate end-to-end detection and response capabilities.

5.10 Secure Decommissioning & Asset Disposal

- Decommissioned devices undergo a three-step data destruction process: cryptographic erase, DoD-standard multi-pass overwrite, and physical shredding of storage media.
- A certified e-waste recycler (ISO 14001 accredited) will handle hardware disposal; chain-of-custody paperwork is tracked in the Asset Register and audited annually.

5.11 Physical Site Security & Access Monitoring

- All primary hardware locations (Hobart HQ, Launceston lab) and remote CareBot deployment sites will implement layered perimeter controls: security fencing, badge-access turnstiles, 24/7 CCTV with motion analytics, and on-site alarm systems.
- A central Security Operations Centre (SOC) will aggregate door-access logs, CCTV events and tamper alerts via an integrated Physical Security Information Management (PSIM) platform. Any anomalous after-hours entry or repeated access failures triggers an immediate alert to both the local site manager and the Head of Security.
- Quarterly drills will test response to physical breaches, including simulated fence cuts and tailgating attempts. Performance metrics (mean time to detect, time to respond, incident resolution rate) are tracked to drive continuous improvement.

5.12 Performance, Capacity & Resilience Planning

- Hardware assets must meet defined Service-Level Objectives (SLOs) for compute, storage and network throughput. Baseline performance metrics are captured during commissioning, with automated capacity monitoring to forecast resource exhaustion three months in advance.
- Disaster scenarios power failure, network outage, extreme temperature are modeled annually. Critical systems (HW-01, HW-03) deploy in a geo-redundant

configuration across Hobart and Launceston to maintain ≥99.95% availability. Switchover procedures are tested quarterly, and failback documented in the DR playbook.
- Mean time between failures (MTBF) and mean time to repair (MTTR) are reviewed monthly; any trend of degrading MTBF triggers hardware refresh planning.

5.13 Maintenance, Calibration & Vendor Assurance

- All CareBots and lab instrumentation follow a preventive maintenance schedule: firmware health checks bi-weekly, mechanical calibration monthly, and full system diagnostics quarterly. Maintenance tickets and calibration certificates are stored in the Asset Management System.
- Approved maintenance vendors must present proof of staff background checks, ISO 9001 quality processes, and cyber-risk assessments before engagement. Contractual SLAs enforce maximum repair turnaround times (48 hrs for CareBots, 72 hrs for lab devices) with financial penalties for non-compliance.
- Vendor performance is scored annually on metrics including on-time delivery, repair quality and security posture. Underperforming suppliers are subjected to remedial action plans or replacement sourcing.

6. Justification and Compliance

These measures reduce the likelihood of compromise for both locally managed and customer-deployed systems. They align with:

- ACSC Essential Eight (Application control, Patch management)
- ISO/IEC 27001:2022
- OAIC's guidelines for securing IoT and medical devices
- The Privacy Act 1988 (Cth)

Failure to secure hardware could result in not only operational disruption but also legal non-compliance, particularly under the Notifiable Data Breaches scheme.

7. Monitoring and Evaluation

- Quarterly hardware security audits will be conducted.
- Audit logs from mobile devices, CareBots, and entry systems will be correlated for anomaly detection.
- Penetration tests on deployed CareBots will be simulated annually.
- Asset inventory and tracking compliance will be measured monthly.

8. Conclusion

Hardware assets form the physical foundation of TanuCare’s service delivery model. Securing them requires a multi-layered approach that combines physical protection, firmware integrity, strict access controls, and vigilant monitoring. These controls will ensure the continued safety, reliability, and legal compliance of TanuCare's health-tech systems while supporting client trust in both domestic and clinical environments.

Section 2.2: Security for Software Assets (Made by Parth Patel)

1. Overview

TanuCare's software ecosystem supports its robotic operations, appointment management platform, internal development pipelines, and secure client communications. Key components include the TanuCare App, backend APIs, robot firmware, CI/CD infrastructure, third-party integrations, and office productivity tools. These systems handle sensitive patient data, real-time commands to CareBots, and interactions with national services like NDIS and Medicare.

Due to their central role and exposure to external interfaces, software assets are a primary attack surface. This section outlines controls to ensure software integrity, prevent exploitation, and maintain operational continuity in accordance with the risks outlined in Section 1.3 and policy directives from Section 1.5.

2. Software Asset Inventory

Asset Code	Description	Function	Risk Level
SW-01	TanuCare App & APIs	Appointment booking, monitoring	High
SW-02	Robot Firmware	Device behaviour, updates	Critical
SW-03	DevOps Platform (CI/CD)	Code deployment, automation	High
SW-04	3rd Party Integrations	NDIS, Medicare	Medium
SW-05	Office Software	Communication, documentation	Medium

3. Threat Landscape

3.1 Code Injection and API Abuse

Exploitation of insecure endpoints in SW-01 could lead to data breaches or unauthorised actions.

3.2 Firmware Backdoors

Firmware (SW-02) might be targeted for backdoors that allow attackers to control robots remotely.

3.3 Uncontrolled Code Pushes

Weak access control or validation in SW-03 can result in insecure builds, production bugs, or backdoors.

3.4 Insecure 3rd Party Dependencies

SW-04 integrations can inherit vulnerabilities from national portals or third-party SDKs.

3.5 Human Error and Misconfigurations

Staff using SW-05 may accidentally expose sensitive files, send credentials, or install malware.

4. **Security Goals for Software Assets**

- Ensure confidentiality and integrity of app interactions and data processing
- Maintain secure DevOps practices across all environments
- Enforce validated firmware updates and access restrictions
- Monitor 3rd party dependencies for security advisories
- Apply Policies P01 (Encryption), P02 (Firmware Security), P03 (Access Control), P05 (Patch Management), P09 (3rd Party Policy)

5. **Proposed Security Measures**

5.1 Secure Software Development Lifecycle (SDLC)

- Mandatory static code analysis before any release (SW-01, SW-03)
- Threat modeling during the design phase
- All developers trained in OWASP Top 10 vulnerabilities

5.2 API and App Hardening (Policy: P01, P03)

- Rate-limiting, input validation, and token authentication enforced on APIs
- Transport Layer Security (TLS 1.3) used across all communications
- End-to-end encryption for in-app video streams

5.3 Firmware Signing and Verification (Policy: P02, P05)

- Signed firmware only, verified before execution (SW-02)
- Checksums and secure boot enforced on CareBots
- Regular firmware security reviews based on MITRE ATT&CK

5.4 DevOps Security (Policy: P03)

- CI/CD pipelines require code review approvals and security test passes
- Git access restricted by roles, with audit logging
- Secrets and credentials stored in vault systems, not in code

5.5 Third-Party Risk Management (Policy: P09)

- Vulnerability assessments of APIs and SDKs used from SW-04
- Contracts must include breach reporting clauses and security SLAs

- Disconnected fallback services prepared for national system outages

5.6 Office Software Controls (Policy: P06, P10)

- Data loss prevention tools on productivity apps
- Auto-expiry of shared documents and file access logs
- Macro execution disabled by default

5.7 Secure SDLC & Code Integrity:

- To embed security from design through deployment, TanuCare will adopt a formal Secure Software Development Lifecycle (SDLC). All projects will begin with threat modeling and a privacy impact assessment OWASP Top 10 coding standards will be enforced via mandatory peer reviews and automated static application security testing (SAST) on every merge. Security gates in the CI/CD pipeline will block any build with high or critical-level findings, and all released binaries will be cryptographically signed to guarantee integrity.

5.8 Dependency & Container Security:

- Third-party libraries and container images will be scanned automatically (daily) using a vulnerability management tool. Critical fixes must roll out within 48 hours of vendor patch release. Only approved, signed images from trusted registries may be deployed. A Software Bill of Materials (SBOM) will be maintained for each service.

5.9 Secrets Management & Runtime Monitoring:

- Application secrets (API keys, certificates) will reside in a centralized vault with automatic rotation every 60 days. Runtime logs and security events will forward to the SIEM for real-time analysis. A Web Application Firewall (WAF) will guard public APIs, and anomaly detection alerts will trigger the Incident Response Plan (Section 1.4).

5.10 API Security & Input Validation:

- All microservices and public-facing APIs will enforce a strict schema validation layer (using JSON Schema/OpenAPI definitions), rejecting requests that deviate from expected data types or contain unexpected fields.
- Rate-limiting and behavioural analytics (burst-detection) on each endpoint will throttle anomalous traffic, with automated blacklisting of repeat offenders.
- A centralized API-gateway will handle authentication, OAuth 2.0 token introspection and JWT signature validation for inter-service calls.

5.11 Secure Architecture & Design Reviews:

- Every new feature or service must undergo a formal security design review prior to development. Reviews include threat modeling (STRIDE/DREAD), data flow analysis and privacy impact assessment.
- A rotating panel of developers, DevOps and security architects will sign off on architecture docs, ensuring separation of duties and no single point of blind-spot risk.
- Exceptions to secure-by-design Principles must be documented, risk-rated and mitigated via compensating controls.

5.12 Containerization & Runtime Protection:

- All container images are built from minimal base OS layers, scanned daily for CVEs, and stored in a private, signed registry.
- Runtime security agents (live-patching, anomaly detection) are deployed to container hosts to identify and quarantine compromised processes within seconds.
- Kubernetes admission controllers enforce PodSecurityPolicies (PSP) that forbid privileged containers, hostPath mounts and escalating capabilities.

5.13 DevSecOps & CI/CD Integration:

- Security tests (SAST, DAST, dependency checks) are mandatory pipeline stages: builds with any critical/high findings are rejected, and developers receive automated issue tickets.
- A Security Champion in each team tracks weekly vulnerability metrics and triages fixes during sprint planning.
- A continuous feedback loop using retrospectives after every security incident drives process improvements, tracked via the DevSecOps dashboard.

5.14 Runtime Application Self-Protection (RASP):

- RASP agents embed into production binaries, monitoring code-injection, SQL injection and deserialization attempts in real time. Detected attacks trigger instant diagnostic dump and safe-mode fallback.
- All RASP incidents are forwarded to the SIEM as high-severity events, auto-escalated into the Incident Response Plan (Section 1.4).

5.15 Observability & Centralized Logging):

- Applications emit structured logs (JSON) and performance metrics to our SIEM and monitoring platform over encrypted channels.
- Logs include transaction IDs, user IDs, error codes, latency timings and authentication events, stored immutably for 90 days.
- Dashboards track KPIs error rates, response times, failed logins and dynamic thresholds trigger high-priority alerts.
- High-severity anomalies automatically generate incident tickets and escalate per the Incident Response Plan (Section 1.4).

- Retrospective analysis of logs feeds root-cause investigations and continuous improvement of security controls.
- Automated correlation of log events with external threat intelligence enriches context and reduces false positives.

5.16 Threat Intelligence & Vulnerability Disclosure:

- The security team subscribes to commercial and open-source threat feeds (e.g., OWASP DB, local CERT alerts, Dark Web monitoring) and ingests them into our SIEM.
- Any vulnerability affecting in-use frameworks or libraries (per our SBOM) is triaged within 24 hours, rated per CVSS v3.1, and assigned remediation SLAs.
- A formal Responsible Disclosure program is published on TanuCare's website, with clear submission guidelines, non-disclosure assurances, and a 30-day SLA for initial response.
- Coordinated disclosure with vendors and customers follows ISO/IEC 29147/30111 processes, ensuring timely patch development and distribution.
- Monthly intelligence reports summarizing critical threats, exploit trends and remediation status are delivered to the CISO and DevSecOps teams.

5.17 Developer Education & Security Champions:

- A Security Champions program designates a trained security advocate in each development team; champions attend monthly workshops on secure coding, threat modeling (STRIDE) and API hardening.
- Champions run quarterly peer-review sessions on injection flaws, auth bypass and insecure deserialization, and maintain a shared library of secure code patterns.
- An internal security portal hosts up-to-date developer guides, cheat-sheets, lab exercises and video tutorials, all refreshed bi-annually with new framework-specific and regulatory content.
- Following any security incident, a mandatory post-mortem workshop documents findings in team retrospectives and updates training materials.
- Participation metrics trainings completed, peer-review issues closed, incident-drill performance are tracked on the DevSecOps dashboard for quarterly reporting.

6. **Justification and Compliance**

TanuCare's software controls align with:

- ACSC's Cloud and Application Security principles
- ISO/IEC 27034-1:2011 (Application Security)
- OWASP Secure Coding Practices
- OAIC and NDB compliance for data protection

These measures reduce the attack surface, protect critical systems, and prevent unintentional data exposure, all of which are essential to trust and legal accountability.

7. **Monitoring and Evaluation**

- Quarterly vulnerability scans and penetration testing of web and mobile apps
- DevOps audit reports reviewed monthly
- Firmware update logs retained and reviewed quarterly
- Vendor security assessments renewed annually

8. **Conclusion**

Software assets are the digital core of TanuCare's care delivery platform. Securing them requires strong development practices, hardened access controls, and close monitoring of third-party dependencies. These measures ensure the software remains secure, resilient, and compliant with national and industry cybersecurity standards.

Section 2.3: Security for Data Assets **(Made by Ravi Savani)**

1. **Overview**

TanuCare manages a significant volume of sensitive and regulated data, including patient health records, biometric sensor data, staff and contractor details, source code, and system logs. These data types are stored across cloud services, local servers, mobile devices, and CareBots deployed in clients' homes. Given the sensitive nature of this information and the organisation's obligations under the Privacy Act 1988 (Cth) and Notifiable Data Breaches (NDB) scheme, securing data assets is paramount.

This section outlines controls to ensure confidentiality, integrity, and availability of data assets throughout their lifecycle. Strategies are informed by the risk register in Section 1.3 and policies P01 (Encryption), P03 (Access Control), P04 (Backup and Recovery), P06 (Security Awareness), and P08 (Logging and Monitoring).

2. **Data Asset Inventory**

Asset Code	Description	Type	Sensitivity
DA-01	Client Health Data	Structured (PII/medical)	Critical
DA-02	Audio/Video Feeds from CareBots	Unstructured (media)	High
DA-03	System Logs & Audit Trails	Structured	Medium
DA-04	Source Code Repositories	Intellectual property	High
DA-05	HR and Financial Records	Structured (internal)	High

3. **Threat Landscape**

3.1 Data Breaches and Leaks

Unencrypted or improperly stored records (DA-01, DA-02) can be exfiltrated through malware, insider misuse, or misconfiguration.

3.2 Integrity Attacks

Tampering with logs (DA-03) or source code (DA-04) could compromise operational integrity or introduce backdoors.

3.3 Insider Threats

Privileged staff with unmonitored access may leak or misuse sensitive data (DA-04, DA-05).

3.4 Ransomware and Data Loss

Health data (DA-01) and HR files (DA-05) may be encrypted by ransomware or lost during cloud outages without backup.

4. **Security Goals for Data Assets**

- Prevent unauthorized access to personal, health, and business-sensitive data
- Preserve data accuracy and verifiability
- Ensure timely recovery in the event of loss or compromise
- Maintain auditable history of data handling activities

5. **Proposed Security Measures**

5.1 Encryption and Access Controls (Policies: P01, P03)

- All PII and health data encrypted using AES-256 in storage and TLS 1.3 in transit
- Role-based access restrictions enforced across all cloud storage buckets and internal drives
- Session-based timeouts and device-bound access tokens for CareBot data streams

5.2 Data Classification and Labelling

- All data tagged by sensitivity (Public, Internal, Confidential, Restricted)
- Labels embedded in file metadata, enforced by DLP tools

5.3 Audit Logging and Monitoring (Policy: P08)

- Immutable logs maintained for all access/modification of DA-01, DA-03, DA-04
- Alerting on unauthorized or suspicious access patterns
- Correlation with SIEM tools to detect anomalies

5.4 Secure Backup and Recovery (Policy: P04)

- Nightly encrypted backups of critical data to geo-redundant cloud storage
- Monthly restore drills with verification for DA-01 and DA-05
- Offline cold storage maintained for legal retention of medical records

5.5 Source Code Protection

- Multi-signature commits enforced for production branches
- Git repositories hosted in private, access-logged repositories
- Secrets management systems used to prevent credential leaks in DA-04

5.6 Insider Risk Management (Policy: P06)

- Periodic behaviour analytics on access to high-risk data
- Confidentiality agreements and disciplinary procedures in place
- Exit workflows trigger data access revocation and device audits

5.7 Data Encryption & Key Management:

- All data at rest (databases, backups, device caches) and in transit must use AES-256 or TLS 1.3. Encryption keys will be stored in a hardware security module (HSM) or vault service, with role-based access and automated rotation every 90 days (Policy P04).

5.8 Backup, Archival & Recovery:

- Daily incremental and weekly full backups of all DA-xx datasets will be stored off-site in encrypted form. Restore tests will be performed quarterly, with documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) as per Policy P05.

5.9 Data Minimization & Retention:

- Only the minimum necessary personal and operational data will be collected and retained. A data-retention schedule will automatically purge records older than their business or regulatory requirement (e.g. 7 years for medical logs) in alignment with Policy P08.

6. **Justification and Compliance**

Data asset controls are necessary to:

- Comply with the Australian Privacy Principles (APPs)
- Support the NDB scheme’s integrity and breach reporting requirements
- Preserve public trust in TanuCare’s AI-enabled care solutions

- Safeguard the competitive value of internally developed IP

These measures adhere to:

- ISO/IEC 27001 Annex A.8 (Asset Management)
- OAIC's Guide to Securing Personal Information
- ACSC's Strategies to Mitigate Cyber Security Incidents

7. Monitoring and Evaluation

- Monthly data access and leak prevention audits
- Quarterly policy compliance reviews and role-based access audits
- Biannual incident response simulations involving data breach scenarios
- Real-time alerting dashboards integrated with endpoint agents

8. Conclusion

TanuCare's data assets are its most sensitive and valuable resources. A strong data security strategy, incorporating encryption, monitoring, role-based controls, and proactive risk management, ensures data remains protected and operations stay compliant. These measures enable the safe use of robotics and remote care technologies in Tasmania's digital health landscape.

Section 2.4: Security for Business Assets (Made by Malay Prajapati)

1. Overview

TanuCare's business assets are fundamental to maintaining trust, continuity, and regulatory compliance. These assets include its reputation, intellectual property, contractual obligations, legal compliance status, and customer relationships. Unlike hardware and software, these are intangible but equally critical to organisational success. Their compromise may not only disrupt operations but also damage public perception and cause irreversible legal consequences.

Business asset protection requires robust governance, policy enforcement, third-party management, and staff accountability. This section identifies risks to TanuCare's business interests and presents security controls aligned with policies P03 (Access Control), P06 (Security Awareness), P07 (Incident Reporting), P09 (Third-Party Integrations), and P10 (Acceptable Use).

2. Business Asset Inventory

Asset Code	Description	Type	Sensitivity
BA-01	Company Reputation	Public trust	Critical

BA-02	Regulatory Compliance	Privacy, NDIS, NDB	High
BA-03	Availability of Care Services	Business continuity	High
BA-04	Intellectual Property (AI Models, Plans)	Proprietary	High
BA-05	Third-Party Relationships	Vendors, partners	Medium

3. **Threat Landscape**

3.1 Reputational Damage

Data breaches or service failures can erode public trust, especially in the health-tech domain (BA-01).

3.2 Legal and Compliance Failures

Failure to meet obligations under the Privacy Act or NDIS guidelines can result in penalties and customer loss (BA-02).

3.3 Service Downtime

Ransomware, DDoS attacks, or infrastructure failures affecting booking systems or CareBot APIs can halt critical care delivery (BA-03).

3.4 IP Theft

Leaked AI algorithms or care workflow systems can give competitors unfair advantage (BA-04).

3.5 Third-Party Risk

Weaknesses in partner systems may introduce vulnerabilities into TanuCare's infrastructure (BA-05).

4. **Security Goals for Business Assets**

- Maintain stakeholder confidence and brand integrity
- Ensure compliance with all health and data regulations
- Guarantee service availability and disaster recovery
- Protect IP and internal documents from theft or unauthorised access
- Monitor and manage third-party cyber risks

5. **Proposed Security Measures**

5.1 Brand Protection and Response

- Proactive breach notifications and public disclosure procedures (BA-01)
- Social media monitoring for incident signals
- Communication officer trained in crisis messaging

5.2 Regulatory Compliance Management (Policy: P07, P09)

- Continuous mapping of internal controls to NDIS and Privacy Act requirements
- Annual audit by independent third-party for compliance scorecard
- Policy P07 ensures that all reportable events are logged and reviewed within 72 hours

5.3 Business Continuity and DRP (Policy: P04)

- Redundant infrastructure for app services and CareBot connectivity
- Monthly tabletop exercises for service interruption scenarios (BA-03)
- Clear RTO and RPO objectives documented and tested quarterly

5.4 Intellectual Property Protection (Policy: P03, P10)

- Role-based access to internal designs, AI models, and workflow blueprints
- NDAs and digital watermarking for confidential project files
- Codebase access limited to need-to-know staff with MFA enforcement

5.5 Vendor Risk Management (Policy: P09)

- Due diligence checklist prior to onboarding any third-party provider
- Contracts must include breach reporting timelines, indemnity clauses, and service-level agreements (SLAs)
- Third-party penetration tests required annually for high-impact vendors

5.6 Security Awareness (Policy: P06)

- Staff training on confidentiality, communication boundaries, and regulatory responsibilities
- Mandatory onboarding and annual refreshers
- Anonymous whistleblowing channel for unethical practices

5.7 Contractual & SLA Management:

- All third-party agreements and service contracts will include comprehensive cybersecurity clauses breach notification within 24 hours, indemnity provisions, and required security controls. Service level agreements must define minimum uptime, incident response times, and performance metrics, with annual contract reviews by the Legal and Compliance teams.

5.8 Cyber Insurance & Financial Risk Transfer:

- TanuCare will maintain a tailored cyber insurance policy covering data breaches, business interruption, and regulatory fines. Coverage limits and terms will be reviewed annually against evolving threat landscapes and asset valuations. The Risk Committee will oversee claim processes and liaise with insurers to ensure optimal coverage.

5.9 Crisis Communications & Brand Recovery:

- A documented crisis-communications plan complete with templated statements and stakeholder notification flowcharts will be tested quarterly via media-drills. A designated communications lead will coordinate messaging to protect brand reputation and maintain public trust.

6. **Justification and Compliance**

These business-focused controls protect TanuCare's strategic value and ensure the company is resilient, trustworthy, and legally sound. In particular, they align with:

- ISO/IEC 27001:2022 governance and compliance controls
- Australian Privacy Principles (APPs)
- ACSC maturity models for essential business operations
- Risk categories highlighted in the OAIC Notifiable Data Breaches guidance

7. **Monitoring and Evaluation**

- Brand audits and customer sentiment reports published bi-annually
- Regulatory self-assessments submitted quarterly to senior management
- Continuous service uptime monitoring via third-party dashboard
- Vendor risk re-evaluation scheduled every 12 months

8. **Conclusion**

Business asset protection at TanuCare involves both strategic foresight and detailed execution. By integrating legal compliance, service continuity planning, and staff accountability into daily operations, the organisation ensures its long-term viability and leadership in the health-tech sector. These controls support ongoing innovation while maintaining stakeholder confidence and regulatory integrity.

Section 2.5: Acceptable Use Policy (AUP) (Made by Parth Patel, Ravi Savani, Malay Prajapati, Md Khalil)

1. **Overview**

The Acceptable Use Policy (AUP) at TanuCare defines the permissible and prohibited activities related to the use of the organisation's IT systems, data, devices, internet access, and communication platforms. Given TanuCare's responsibility for managing sensitive health information, operating robotic systems, and ensuring regulatory compliance, all employees, contractors, and third-party users must adhere to these guidelines.

This AUP supports the enforcement of broader cybersecurity strategies laid out in Section 1.5 and directly aligns with Policies P03 (Access Control), P06 (Security Awareness), P07 (Incident Reporting), and P10 (Acceptable Use).

2. **Scope**

This policy applies to:

- All full-time, part-time, and temporary employees
- Contractors and third-party vendors with system access
- Interns, volunteers, and university collaborators

It covers all use of:

- Workstations, laptops, and mobile devices
- Company email, messaging platforms, and software
- Internet usage during working hours or on company devices
- Access to health data, CareBot systems, or internal applications

3. **Acceptable Use Guidelines**

3.1 Permitted Use

- Use of company devices and software for legitimate work-related tasks
- Access to data only as needed for assigned duties
- Communication via authorised platforms (e.g., Microsoft Teams, Outlook)
- Remote work access through VPN and MFA-secured channels

3.2 Prohibited Activities

- Accessing, storing, or distributing illegal, offensive, or unapproved content
- Sharing login credentials or leaving devices unattended without lock screens
- Connecting personal devices to production networks without approval
- Using company resources for personal financial gain or side-businesses
- Bypassing security protocols, including firewalls or endpoint protections

3.3 Email and Communication

- All emails must use professional language and tone
- Users must not click suspicious links or download attachments from unknown sources
- Mass communications or forwarding chain emails are prohibited unless authorised

3.4 Software and Applications

- Only approved applications from the internal software catalogue may be installed
- Users may not modify system settings without permission from IT
- All software updates must be installed when prompted

3.5 Physical Device Use

- Devices must be locked when unattended
- Lost or stolen devices must be reported within 24 hours (Policy: P07)
- USBs and external drives must be scanned before use

3.6 Bring Your Own Device (BYOD) Controls:

- All personal devices used for TanuCare work must enroll in the corporate MDM system, enforce full-disk encryption, pass quarterly compliance scans, and support remote wipe on employee off-boarding.

3.7 Application & External Media Management:

- Only software from the approved corporate application registry may be installed. USB ports and removable media are locked down at the endpoint; any external files must be scanned for malware before mounting.

3.8 Network & Communication Use:

- All remote access requires VPN with MFA. Prohibited services (e.g. P2P file-sharing, anonymizers) are blocked at the firewall, and unusual traffic volumes trigger automated alerts.

3.9 Policy Awareness & Exceptions:

- Employees must complete AUP training upon hire and annually thereafter. Any exception to the AUP must be documented with manager approval and reviewed each quarter.

4. **Monitoring and Enforcement**

- All user activity may be monitored in accordance with Australian privacy laws
- Logs will be maintained and reviewed regularly (Policy: P08)
- Violations will result in disciplinary action, including potential termination or legal referral
- Severity tiers: Minor (warning), Moderate (access restrictions), Severe (termination/legal action)

5. **User Responsibilities**

- Read and understand the AUP upon onboarding
- Complete mandatory security awareness training (Policy: P06)
- Immediately report suspicious activity or breaches (Policy: P07)
- Ensure strong passwords and responsible device usage

6. **Justification and Alignment**

A clearly defined AUP ensures:

- Reduced risk of human error leading to breaches
- Better enforcement of access controls and legal compliance
- Transparent expectations for internal and external users

This policy supports ISO/IEC 27002 control A.9 (User Responsibilities), aligns with the Australian Privacy Principles (APP 6 and 11), and reduces insider threats.

7. **Monitoring and Evaluation**

- Quarterly AUP awareness checks and spot audits
- Annual staff re-signing of the policy
- Metrics tracked: policy violations, device misuse reports, phishing simulation results

8. **Conclusion: Summary of Cybersecurity Foundations**

TanuCare’s Acceptable Use Policy sets clear expectations and boundaries for how technology and data may be used within the organisation. By educating users, enforcing compliance, and integrating monitoring mechanisms, the AUP reduces the risk of insider threats, accidental breaches, and non-compliant behaviour while fostering a security-conscious culture.

Conclusion

TanuCare's cybersecurity policy provides a comprehensive framework to address the unique security challenges faced by a modern health-tech and robotics enterprise. Through detailed risk analysis and a structured policy-based response, the organisation is equipped to protect its critical hardware, software, data, and business assets against evolving cyber threats. The use of structured controls, aligned with national standards such as ISO/IEC 27001, ACSC Essential Eight, and the Privacy Act 1988 (Cth), ensures both operational continuity and regulatory compliance.

Each policy, from encryption and firmware integrity to incident response and acceptable use, reflects a deep understanding of the company's threat profile and strategic goals. The individual asset-focused sections demonstrate how these high-level controls are operationalised in day-to-day practices, enabling secure deployment of CareBots, protection of sensitive patient data, and the delivery of reliable, ethical care solutions across Tasmania.

This report demonstrates that cybersecurity is not just a technical concern but a core business priority at TanuCare. By embedding security into the organisation's culture, systems, and procedures, TanuCare can continue to innovate confidently in the health robotics space while safeguarding the wellbeing and privacy of its users.

References

- Australian Government. (1988). Privacy Act 1988. Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/C2004A03712/latest
- Australian Cyber Security Centre. (2017). Essential Eight Maturity Model. Australian Government. Retrieved from https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-maturity-model
- Australian Cyber Security Centre. (2022). PROTECT – Essential Eight Maturity Model (November 2022). Australian Government. Retrieved from https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28November%202022%29.pdf
- International Organization for Standardization. (2011). ISO/IEC 27034-1:2011 Information technology Security techniques Application security Part 1: Overview and concepts. Retrieved from https://www.iso.org/standard/44378.html
- International Organization for Standardization. (2014). ISO/IEC 29147:2014 Information technology Security techniques Vulnerability disclosure. Retrieved from https://www.iso.org/standard/45170.html
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information technology Security techniques Information security management systems Requirements. Retrieved from https://www.iso.org/standard/82875.html

- International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information technology Security techniques Code of practice for information security controls. Retrieved from https://www.iso.org/standard/75652.html
- MITRE Corporation. (2024). ATT&CK®: Adversarial Tactics, Techniques, and Common Knowledge. Retrieved from https://attack.mitre.org/
- National Institute of Standards and Technology. (2012). NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Open Web Application Security Project. (2024). OWASP Top Ten. Retrieved from https://owasp.org/www-project-top-ten/
- Office of the Australian Information Commissioner. (2024). Data breach preparation and response. Retrieved from https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response
- Office of the Australian Information Commissioner. (2024). Notifiable data breaches. Retrieved from https://www.oaic.gov.au/privacy/notifiable-data-breaches