Policy Name	Dept: Clinical	Dept: Engineering	Dept: Product	Dept: Customer Support	Dept: HR	Dept: Finance	Dept: Legal & Compliance	Dept: Marketing	Dept: Sales	Rationale
Acceptable Use	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Assigned to all staff. Policy targets prohibited behaviours when using organisational systems and data. Legal must understand this policy for legal purposes.
Access Control	Yes - Manager	Yes - Staff	Yes - Manager	No	No	No	Yes - Staff	No	No	Creating, modifying, and removing access to organisational systems and data using the least privelage philosophy is a technical control. Product Manager directly manages platform, system, and application access design and controls. Legal must understand this policy for legal purposes.
Artificial Intelligence	Yes - Manager	Yes - Staff	Yes - Staff	Yes - Manager	Yes - Manager	Yes - Staff	Yes - Staff	Yes - Manager	Yes - Manager	AI is a global emerging technology and all managers and most staff must understand the AI risk and ensure AI technologies are utilised in a secure, ethical, and legally compliant manner.
Asset Management	No	Yes - Staff	No	No	No	No	Yes - Manager	No	No	Technical staff need to ensure all information assets are identified, recorded, and managed throughout their lifecycle. Legal must understand this policy for legal purposes.
Backup	Yes - Manager	Yes - Staff	Yes - Staff	No	No	No	Yes - Manager	No	No	Technical staff must ensure the CIA of organisational data by implementing a structured backup process.. Legal must understand this policy for legal purposes.
Buisness Continuity	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Business continuity impacts all operational areas, especially in a remote, SaaS environment and requires coordinated action, involving all departments.
Change Management	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Applies to all department managers as a buisness wide secure, structured and predictable process is vital for day-to-day buisness.
Code Of Conduct	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	All staff must abide by the organisational code of conduct policy.
Data Classification	Yes - Manager	Yes - Manager	Yes - Manager	No	No	Yes - Manager	Yes - Staff	No	No	Clinical, Engineering, Product, Customer Support manager. These teams work directly with PHI, PII, or sensitive business data, so they need to classify it properly to protect it and meet legal requirements. Legal must understand this policy for legal purposes.
Data Protection	Yes - Manager	Yes - Staff	Yes - Staff	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Staff	Yes - Manager	Yes - Manager	Clinical, Engineering, Product, Customer Support (Manager) regularly handle PHI/PII. Legal must understand this policy for legal purposes.
Data Retention	Yes - Manager	Yes - Staff	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Staff	No	No	Clinical, Engineering, Product, Customer Support (Manager) regularly handle PHI/PII. Legal must understand this policy for legal purposes.
Disaster Recovery	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	For such a small organiseation all staff must adhere to the disaster recovery policy for buisness continuity
Document Control	Yes - Manager	Yes - Manager	No	No	No	No	Yes - Staff	No	No	Technical staff must ensure all documents are managed through their entire life cycle. Legal must understand this policy for legal purposes.
Encryption Policy	No	Yes - Staff	Yes - Staff	No	No	No	Yes - Manager	No	No	Data at rest and transit should be encrypted and is a technical control. Legal must understand this policy for legal purposes.
Incident Response	Yes - Manager	Yes - Staff	Yes - Manager	Yes - Manager	Yes - Manager	No	Yes - Staff	No	No	Incident response is generally assigned to the technical team with customer service involved for intelligence purposes. Legal must understand this policy for legal purposes.
ISMS Plan	Yes - Manager	Yes - Staff	Yes - Staff	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Staff	Yes - Manager	Yes - Manager	Most staff and all managers must understand and adhere to the organisation's core information security expectations, regardless of role.
Info Security Policy ISO 27001	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	A commitment to protecting information assets through risk identification is applicable to all staff.
Info Security Risk Management Framework	Yes - Manager	Yes - Staff	Yes - Staff	Yes - Manager	Yes - Staff	Yes - Manager	Yes - Staff	Yes - Manager	Yes - Manager	All managers and most staff must understand the risk framework and impliment the ISMS framework into day to day practices.
Logging and Monitoring	No	Yes - Staff	Yes - Manager	No	No	No	Yes - Manager	No	No	Technical controls, assigned to technical staff. Legal must understand this policy for legal purposes.
Vulnerability Management	No	Yes - Staff	Yes - Manager	No	No	No	Yes - Manager	No	No	Technical control, assigned to technical staff. Legal must understand this policy for legal purposes.
Network Security Policy	No	Yes - Staff	Yes - Manager	No	No	No	Yes - Manager	No	No	Technical control, assigned to technical staff. Legal must understand this policy for legal purposes.
Password Policy	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	Yes - Staff	All staff must understand the organisations password policy.
Personal Data Management	Yes - Manager	Yes - Staff	Yes - Staff	Yes - Manager	No	No	Yes - Staff	No	No	Technical staff PHI/PII databases. Customer support must understand the use of PII of their customers. Legal must understand this policy for legal purposes.
Physical Security	No	No	No	No	No	No	Yes - Manager	No	No	With no physical premisis there is no need for a physical security policy. Legal must understand this policy for legal purposes.
Responsible Disclosure	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	Yes - Manager	No	Yes - Staff	Yes - Manager	Yes - Manager	Inbound vulnerability disclosure should be handled by the technical team. Legal must understand this policy for legal purposes.
Software Development	No	Yes - Staff	Yes - Manager	No	No	Yes - Manager	Yes - Manager	No	No	Technical controls, assigned to technical staff. Legal must understand this policy for legal purposes.
Vendor Management	No	Yes - Manager	Yes - Manager	No	No	No	Yes - Staff	No	No	Third party technology integrates with company IT and are handled by the technical department. Legal must understand this policy for legal purposes.