Information Security Policy

<table>
<tr><th colspan="3">Document Number</th><th>Version Number</th><th colspan="2">Information Classification</th></tr>
<tr><td colspan="3">GP 500-2 (4)</td><td>4.0</td><td colspan="2">For Office Use Only</td></tr>
<tr><th colspan="4">Approved by</th><th colspan="2">Date</th></tr>
<tr><td colspan="4">General Manager, IT &amp; Risk</td><td colspan="2">03/07/2023</td></tr>
<tr><th colspan="4">Document Owner</th><th colspan="2">Incumbent</th></tr>
<tr><td colspan="4">Manager, Cyber Risk & Governance</td><td colspan="2">Jed Hitchcock</td></tr>
<tr><th colspan="6">Document History</th></tr>
<tr><td><b>Date</b></td><td><b>Version</b></td><td colspan="2"><b>Version Details</b></td><td><b>Author</b></td><td><b>Reviewer/s</b></td></tr>
<tr><td>03/07/2023</td><td>4.0</td><td colspan="2">Updates to Principle and Responsibilities Section, updated format.</td><td>Manager, Cyber Risk & Governance</td><td>GM, IT and Risk</td></tr>
</table>

Contents

1. Purpose

Information is an important asset for Maxima, playing a vital role in supporting business processes and customer services, in contributing to operational and strategic business decisions, and in conforming to legal, statutory and contractual requirements. Maxima recognises the importance of Information Security in supporting Maxima's business objectives and seeks to ensure the Confidentiality, Integrity and Availability of Information, Data, Technology and Information Assets are adequately protected.

The aim of this policy is to set Information Security objectives for the protection of Maxima's Information and Technology Assets and the management of Information Security risks.

2. Scope

This policy applies to:

- All Maxima Workers (part-time, full-time, casual Employees, Volunteers, Contractors, Trainees) who use and/or have access Maxima Information Assets and Maxima's ICT environment.
- All Maxima physical locations, including head office, metropolitan, regional and remote sites that access the Maxima ICT Environment.
- The Maxima ICT Environment including technology that processes, stores or transmits Information and/or Data.
- Third Parties who use and/or have access Maxima Information and/or Maxima's ICT Environment; or store, process or transmit Maxima Information and/or Data.

3. Principles

Maxima's Principles in achieving the Information Security objectives are:

3.1 Trust

Maxima's handling and management of Information is to be trustworthy by ensuring that Information is accurate, relevant, timely, available and secure. This requires:

3.1.1 Embedding a culture of accountability and responsibility for the Confidentiality, Integrity, Availability, Safety and Reliability of Maxima's Information Assets and Systems.
3.1.2 Enabling our people to take accountability for their use of Information in their day-to-day role.
3.1.3 Integrating Information Security risk management principles into our planning and decision-making.
3.1.4 Achieving, maintaining and continuously improving compliance with recognised Information Security Standards and frameworks.

3.2 Transparency

Maxima's handling and management of Information is to be transparent and clear to all parties. This requires:

3.2.1 Engaging with the business to garner feedback on our Information Security Management System (ISMS) and Information Security program.
3.2.2 Providing engaging and appropriate Information Security training across Maxima to ensure an understanding of the requirements of Maxima's approach to Information Security.
3.2.3 Providing clear and direct guidance on our expectations for the protection and use of all Information, including internal, Third Party, personal and electronic Data.
3.2.4 Keeping stakeholders and customers informed of how their Information and Data is being protected and used.

3.3 Privacy

Personal Information entrusted to Maxima must remain private and protected in accordance with legislation, contractual obligations and customer expectations. This requires:

3.3.1 Understanding the root causes of Information Security events and incidents to continuously improve.
3.3.2 Understanding our Information Security objectives and legislative and contractual environment to ensure it is accurately represented by the ISMS and supporting policies and documentation.

3.3.3 Empowering our people to take responsibility in our Information secure culture and report any concerns or risky behaviours they witness.

3.4 Value

Maxima recognises its Information is valued and accordingly treats it as a strategic asset. This requires:

3.4.1 Proactively measuring our ISMS to enable reporting of the right Information to the right people.
3.4.2 Classifying and handling Information according to its value.
3.4.3 Critically reviewing our ISMS to find positive ways of continually improving and developing it.
3.4.4 Creating innovative ways of communicating our commitment and leadership in Information Security within our community and industry.

4. Objectives

Maxima's Information Security objectives are:

4.1 Our customers and stakeholders trust us to protect the Privacy, Confidentiality, Integrity and Availability of their Information and our technology.
4.2 Information and Technology Assets are managed in line with legislative, regulatory and contractual requirements.
4.3 A security aware culture underpins business resilience to information security and privacy threats and aids in recovering quickly when incidents occur.
4.4 Information security decisions are driven through principles and a pragmatic risk-based approach to best practice.
4.5 Mature information security and privacy practices are seen as an enabler of innovation, growth and safe business operations.

5. Roles and Responsibilities

The effective implementation of this policy requires the commitment of all personnel. Further definition of roles can be found in the Information Security Management System (ISMS) Manual.

Role	Responsibilities
Risk and Compliance Committee	• Providing oversight of cyber risk and audit findings to ensure appropriate resources are in place to achieve and maintain Maxima's security objectives.
Executive & Leadership Group	• Each individual member of the Executive and Leadership Group has day to day responsibility and accountability for the management of Information Security in their business. • Providing resources to ensure the requirements of this policy and supporting documents are successfully implemented within their business unit. • Understand and manage the risks associated with the systems and Information required for the successful execution of their processes and achievement of business objectives.
General Manager, IT & Risk	• Has ultimate responsibility for the ISMS within Maxima. Key responsibilities are: ○ Sponsoring and supporting the ISMS within Maxima. ○ Providing strategic direction to the ISMS. ○ Chairing the relevant governance groups and committees. • Has overall responsibility for the content of this policy and its operation in Maxima
Line Managers	• Ensuring this policy and any supporting documents are successfully implemented and communicated to their team. • Ensuring that all team members achieve appropriate Information Security training and awareness.

	• Monitoring compliance of implementation within their teams and highlighting opportunities for improvement and/or potential constraints to implementation.
Information Asset Owners	• Assessing the value of information assets and classifying them according to their level of criticality and sensitivity. • Involvement in the identification, assessment, and treatment of risks. • Treating identified risks as per the risk management methodology. • Involvement in audit and review processes to ensure that appropriate controls are applied to their information assets. • Involvement in coordinating corrective actions for security weaknesses detected. • Endorsing appropriate user privileges and authorising access and changes to the system.
All Maxima Employees	• All employees, contractors, subcontractors, and volunteers undertaking Maxima business activities are required to: ○ Comply with all applicable policies, standards, procedures and supporting documents, and to seek guidance in the event of uncertainty as to its application. ○ Securely handle Information according to its classification. ○ Complete Information Security awareness training relevant to their role and in accordance with expected timeframes. ○ Report any suspicious events or Information Security incidents in accordance with incident management policies and processes.
Third Parties	• When handling Maxima information, accessing systems and/or providing ICT services to Maxima, the third party is responsible for complying with this and other Maxima policies if their contractual requirements specify it.

6. Communication

6.1 Information about this policy will be provided in a timely manner to inform managers, employees and workers.
6.2 A copy of this policy will be maintained and made available through the Maxima Intranet.
6.3 A copy of this policy will be included in onboarding for new staff.

7. Measurement and Evaluation

7.1 This policy will be reviewed annually by the document owner or whenever significant change occurs.
7.2 The effectiveness of this policy will be measured through a KPI reported quarterly to the Risk and Compliance Committee.

8. Compliance

8.1 This policy defines the minimum requirements for Maxima.
8.2 Exceptions to policy requirements must be requested through the General Manager IT & Risk and will be considered on case-by-case basis. Exceptions may be reported to Executive and or the Risk and Compliance Committee and/or the Information Security Management Group for monitoring, direction and escalation as needed.
8.3 Any Worker found in breach of this policy, including its requirements, may be subject to disciplinary action.
8.4 Any Third Party found to be in breach of this policy may have their services terminated.

9. Definitions

Availability means Information Assets are readily available when required by authorised personnel.

Confidentiality means access to Information is restricted to authorised individuals, entities, or processes; and Information is secure from unauthorised individuals or entities.

Contractor means someone that is temporarily employed by Maxima on a contractual basis.

Cyber Security is synonymous with Information Security.

Data means facts and figures suitable for interpretation, processing or communicating.

Employee means people that are directly employed by Maxima.

ICT Environment means the ICT Environment including networks, operating systems, applications, Information, Data, processes and physical hardware and externally hosted services and Information Assets managed by Maxima.

Information Asset means a logical grouping of Information that has value to the organisation, typically this is grouped at the system level.

Information Security means the measures used to protect and preserve the Confidentiality, Integrity, and Availability of Information and Technology Assets. It is synonymous with Cyber Security.

Information means Data grouped or contextualised and has a recognised value and risk.

Information Security Management System (ISMS) means the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and continuously improve Information Security.

Integrity means safeguarding the accuracy and completeness of Information and Data typically in the context of Information Assets.

Privacy has the same meaning as defined by the Office of the Australian Information Commissioner, which in summary means a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination.

Technology Assets means software or physical assets which provide Technology to Maxima and its staff.

Third Parties means a third party who delivers services to or on behalf of Maxima.

Worker means a person who carries out work in any capacity for Maxima, including work as an employee; a contractor or subcontractor; an employee of a contractor or subcontractor; an employee of a labour hire company assigned to work at Maxima; an employee of Maxima assigned to work at another host employer as labour hire; an apprentice or trainee; a student gaining work experience; or a volunteer.

Volunteer is synonymous with Worker for the purposes of this policy.

10. Key Associated Documents

- Acceptable Use Policy (GP 218-2)
- ISMS Manual (GP 500-1)
- Privacy Policy (GP 252-1)
- Risk Management Procedure (GP 101-1)

11. References

Maxima's commitment to Information Security is asserted through ongoing certification with the following standards and accreditations which aid in informing Maxima's Information Security requirements and obligations:

- ISO 9001:2015 Quality Management
- ISO 45001:2018 Occupational Health and Safety
- ISO 27001:2013 Information Security
- National Standards for Disability Services
- Group Training Organisation (GTO) National Standards
- National Disability Insurance Scheme (NDIS) Quality Framework
- Department of Education, Skills and Employment - Right-Fit-For-Risk (RFFR)

For a listing of the legislation for which Maxima comply with, refer to the *Legal and Other Requirements Register*.

12. Appendices

- Nil