Information Security Policy Statement

INTRO	Potentiate Australia Pty Ltd is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our clients, employees, suppliers and for the communities in which we operate. Finding the right balance between information security risk and business benefit enhances business performance and minimises potential future exposures.
OVERALL OBJECTIVES	It is the policy of Potentiate Australia to: • Ensure confidentiality, integrity, and availability of Potentiate's IS systems • Identify, communicate, and manage the responsibilities of users and their obligations to help protect corporate information and systems • Protect Potentiate from business damage or legal liability and the inappropriate use of IS systems and information. • Comply with the needs of the regulatory bodies and relevant legislation.

ASSOCIATED TARGETS	**Ensure confidentiality, integrity, and availability of Potentiate's IS systems** • Information shall be protected against unauthorised access. • Confidentiality of information is maintained. • Information is not disclosed to unauthorised persons through deliberate or careless action. • Integrity of information through protection from unauthorised modification. • Availability of information to authorised users when needed. • Business continuity plans are developed, maintained, and tested **Identify, communicate, and manage the responsibilities of users** • Information security training is available and mandatory for all employees and where applicable tailored for individual roles • Human Resources policies define and assign information security roles and responsibilities throughout the organization. • Educate staff to allow them to independently make informed decision with regards to the secure handling of IT assets and information which is owned by Potentiate Australia Pty Ltd within the framework of the information security policies. **Protect Potentiate from business damage or legal liability and the inappropriate use of IS systems and information.** • Ensure the ability to identify and investigate fraudulent IS related activities and co-operate with relevant legal agencies. • Contractual arrangements or formal agreements with clients, third party service providers, contractors and consultants include all relevant information security requirements **Comply with the needs of the regulatory bodies and relevant legislation.** • Relevant legislative, regulatory, and business requirements are met Any individual dealing with information at Potentiate, no matter what their status (e.g. employee, contractor, or consultant), must comply with the information security policies and related information security documents. The policy applies to all information, computer and network systems governed, owned by and/or administered by Potentiate Australia Pty Ltd.

COMPLIANCE AND CERTIFICATION	Potentiates manages its systems via security controls. The IT operational controls address certain aspects of Information Security specifically and in addition non-IT information assets are included and protected under the Information Security Management System (ISMS). As part of the overall technical and security measures Potentiate is certified with **ISO 27001** requiring that management: • Adopt an overarching management process to ensure that the information security controls are designed and continue to meet the organization's information security objectives and needs on an ongoing basis. • Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable • Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts An independent external auditor tested the Potentiate controls as part of the ISO 27001 certification. This included any controls that the organization deemed to be within the scope of the ISMS which was inclusive of physical security, HR and assets control. The regular audit schedule requires in depth review of the controls that have been implemented and are operating effectively. Management has determined the exhausted scope of the ISMS for certification purposes.

BESTPRACTICE CERTIFICATION
ISO27001
INFORMATION SECURITY MANAGEMENT SYSTEM

Potentiate achieved ISO 27001 – Information Security Certification in February 2017.

Potentiate was re-certified to ISO 27001 on 18th February 2020 after completing the Re-Certification Audit.