Information Security Policy Statement

It is the policy of Potentiate to ensure:

- 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.
- Information security training and ongoing awareness programs will be completed by all staff.
- All suspected breaches of information security shall be reported and investigated.
- Contractual arrangements or formal agreements with clients, third party service providers, contractors and consultants meet all relevant information security requirements
- Any individual dealing with information at Potentiate, no matter what their status (employee, contractor, or consultant), must comply with the information security policies and related information security documents.

The objectives and associated targets are to:

- Meet relevant legislative, regulatory and business requirements
- 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.

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).

Business continuity planning and physical security are designed and maintained to ensure the protection of systems and data. The Potentiate Human Resources policies define and assign information security roles and responsibilities throughout the organization.

As part of the overall technical and security measures Potentiate is certified to ISO 27001 requiring that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts.
- 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; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security objectives and needs on an ongoing basis.

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 asset 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.

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.

© Potentiate 2020