Information Security Policy

Policy Statement

Acceleraate Ltd is committed to information security and protecting the confidentiality, integrity, and availability of all the information assets that we hold within the business.

The SLT is committed to the implementation, ongoing management, and maintenance of the ISMS in order to support the objectives of the business.

The purpose of this commitment is to preserve:

- Competitive advantage,
- Profitability,
- Legal, regulatory, and contractual compliance, and
- Commercial image and reputation.

This policy sets out our commitment, to ensure the information we hold is kept secure. Our information security requirements are aligned with the goals of the business, our strategic business plan, and our risk management framework. All of these provide the context for identifying, assessing, evaluating, and controlling any information related risks through the risk management framework and security framework.

Our commitment to information security is governed by our Information Security Forum (ISF), which is formed in part by, and reports to, the SLT.

1. Purpose

The purpose of this document is to define the framework and the requirements of the organisation for compliance with all information security policies, standards, processes, guidelines, and applicable laws and regulations, to ensure the confidentiality, integrity, and availability of the relevant information assets.

1.1 Scope

This policy applies to all Acceleraate directors, employees, officers, as well as contractors under Acceleraate's direct supervision ("Colleagues"), who may access or make use of the organisation's information resources and systems. The policy also covers any third parties who intend to carry out any work for or on behalf of Acceleraate Limited. Any data that is classified as Personal Data must be processed in compliance with the Data Protection Act 1998, and Acceleraate's data protection and information security policies.

1.2 Information Security Objectives

The SLT will demonstrate leadership and commitment with respect to the Information Security Management System (ISMS) by ensuring the information security policy and the information security objectives are established and are comparable with the strategic direction of the organisation.

The objectives are:

- To protect the Company's information assets in terms of their confidentiality, integrity, and availability to minimise security related incidents, near misses or disruptions to the business,
- Maintain compliance with ISO/IEC 27001 standard,
- Submit to ISO 27001 audit,
- To align information security objectives with the longer-term business objectives of the Company,
- To specify information security roles and responsibilities and ensure competency to support delivery,
- To maintain legal regulatory, statutory, and contractual requirements,
- To provide security assurance to colleagues, clients, partners and other third parties.

1.3 Ownership & Responsibilities

This policy is owned and maintained by Acceleraate Ltd and can be amended with or without notice from time to time at our discretion.

All colleagues and third parties are expected to comply with:

- Information Security Policy,
- Security policies, procedures & guidelines which form a part of the security framework,
- Statutory & contractual requirements, as appropriate to the work that they do.

The SLT will discuss the security framework when (a) either items are raised to it by the director responsible or (b) when any executive member wishes to discuss its operation. Any decisions made at SLT which affect the security framework will be communicated to colleagues and third parties with documentation updated within 7 days.

Third parties will not be expected to comply with any changes to this document until they have been provided with such changes in writing and granted a reasonable period (not to exceed 90 days) to comply with such changes.

This policy will be comprehensively reviewed by Acceleraate Ltd and updated at least once per year.

2. Information Security Policy

Acceleraate Ltd is committed to:

- Reviewing and assessing the effectiveness of the risk management criteria and subsequent treatment plans
- Developing, assessing, and implementing controls, measurable policies, and practices in accordance with the organisation's structure, responsibilities, and governance
- Ensuring that defined service level agreements and measurable services are provided to its clients to provide information security and customer satisfaction
- Ensure its supply chain supports Acceleraate Ltd in its aims
- Implementing, maintaining, and evaluating effective Business Continuity and Disaster Recovery plans relevant to the organisation and its client facing requirements
- Complying with relevant legal and regulatory requirements relevant to its ISMS
- Setting and monitoring relevant measures of effectiveness of its security arrangements
- Continually improving the effectiveness of the ISMS

The ISMS is designed to comply with ISO27001:2013 and we intend to maintain such compliance.

2.1 Management Review

The ISF is responsible for carrying out management reviews in line with the ISO 27001 standard.
The review process focuses on:

- Improving the organisation's assessment of the risks to information security, including updating the risk assessment and risk treatment plan

- Modifying or improving the policies and procedures for managing information security, including improvements to how effectiveness is measured
- Modifying or improving its control objectives and controls to ensure that they are adequately focused on the identified risks and respond to internal and external risks that may impact the security framework, including changes to contractual obligations
- Improving the allocation of resources and responsibilities
- Formulating and agreeing any changes to the information security policy, which would be necessary, to give effect to any improvements identified
- Third parties who fall within the scope may be subject to compliance review against this Policy and will be required to complete an assessment form. Any potential risks that are identified will then need to be mitigated before commencing any works

2.2 Security Access & Training

Colleagues with access to information assets and information processing facilities will be educated on their information security responsibilities.

- Education will be provided at induction so that new colleagues completely understand their responsibilities in the protection of information assets and information processing facilities.
- Colleagues will be provided with ongoing security education and support.
- Acceleraate will provide annual refresher courses and other security related materials to regularly remind colleagues about their obligations with respect to information security. The refresher course will be validated by assessment with a pass score.
- The security responsibilities of third parties shall be made clear at an early stage of the contract.

2.3 Risk Acceptance Criteria

In situations to be determined by SLT, the acceptance of a risk situation shall be granted to allow non-compliance with information security controls. Risk acceptance shall only be used in exceptional situations allowing non-compliance for a specific period. A director shall approve all risk acceptances before non-compliance can ensue. However, in exceptional situations, where risk acceptance is required, approval shall be given by one of the Directors and later confirmed by the SLT. Post reviews of all emergency approvals shall be carried out by the SLT.

2.4 Continuous Improvement

Acceleraate aspires to continually improve its security framework. Improvements to the framework will be discussed during the ISF meetings. Additionally, there will be – at minimum – a formal annual review conducted.

2.5 Information Security within Projects

Projects that involve the handling and sharing of information will be subject to a Risk Assessment which will be undertaken by the project owner with the support of information security qualified colleagues. The Risk Assessment will consider all potential internal and external mitigating factors that may influence the information involved.

Projects that impact on the privacy of individuals will also require a privacy impact assessment to identify and document appropriate governance controls required to manage the privacy risks associated with new or changed processes that involve personal data.

Where a project does not involve information or personal data, then a judgement call should be made as to whether an assessment is required. This reasoning will be documented.

3. Information Security for Third Parties

3.1 Processes and Procedures

- The Third Party will maintain a corporate Information Security Policy defining responsibilities and setting out the Third Party's approach to information security. The Information Security Policies should follow Information Security programs that are based on ISO 27001 or similar frameworks e.g. PCI DSS.
- The Third Party will agree to provide Acceleraate Limited with copies of its security policies on request and evidence of compliance with any of the standards demonstrated by the Third Party e.g. ISO 27001, CSTAR, PCI DSS etc.

3.2 Human Resources

- A dedicated Information Security role should be defined and assigned to an individual in the company and these details communicated to Acceleraate Limited. This individual will act as the primary contact for all Information Security matters.
- The Third Party will ensure that information security roles and responsibilities of all employees (and subcontractors) are clearly defined and documented.

- The Third Party will have a comprehensive disciplinary policy, code of conduct & work rules directive in force.
- The Third Party will ensure that background checks such as BPSS are conducted at the Third Party's cost and within a reasonable period. Checks will be completed prior to any personnel commencing provision of services.
- The Third Party will ensure that a written policy exists and is followed for pre-employment screening and that screening status and results are fully collated and kept on record. Acceleraate Ltd may request a screening status be made available for audit and compliance purposes.
- The Third Party will ensure that all personnel enter a written contract of employment under which they agree to adhere to all policies, rules and procedures including all information protection policies.
- The Third Party will hold structured briefings with respect to security awareness and knowledge focusing on the risks resulting from poor information security, and legal and regulatory requirements to protect information.
- The Third Party will conduct security reviews in accordance with the requirements set out in this Policy document.

3.3 Compliance & Asset Management

- The Third Party will conduct security reviews in accordance with the requirements set out in this Policy document.
- The Third Party will ensure that Acceleraate Ltd information is classified in terms of its value, legal requirements, sensitivity, and criticality. The Third Party will also ensure that an appropriate set of procedures for information labelling and handling is developed and implemented in accordance with the classification scheme.
- All information assets used to process Acceleraate Ltd information must be recorded in a maintained inventory. The Third Party will ensure that any media used to record, store or process Acceleraate Ltd information as part of the Services, including hard copies of documents, and laptops are securely handled, transported, and encrypted and that their use is authorised.
- The Third Party will always ensure that it maintains and abides by an appropriate Data Protection Policy to safeguard Acceleraate Ltd information in accordance with the terms of the contract and the Data Protection Act 1998 (and any amendment thereto to or replacement thereof) and any other applicable statute, regulation or industry code.

- Where any Acceleraate Ltd information is intended to be transferred, stored, or processed outside of the UK, EU or EEA, the Third Party will first obtain permission in writing from Acceleraate Ltd before doing so.
- The Third Party will ensure that appropriate retention and secure deletion/destruction policies and procedures are in place for all Acceleraate Ltd information held. Acceleraate Ltd may require a copy of the policies and procedures.
- The Third Party will notify Acceleraate Ltd immediately in the event of data loss or data breach detailing severity of the exposure.
- The Third Party will not make unauthorised copies of Acceleraate Ltd information

4. Policy Review Process

Acceleraate is committed to continually review and improve all of our policies, and may make changes at any point. At the very least, all policies are reviewed annually and will be issued to all Acceleraate directors, employees, officers, as well as contractors under Acceleraate's direct supervision ("Colleagues").

5. Dispensations

In case of any dispensations or deviations from this document please contact security@acceleraate.com

6. Enforcement & Consequences

Non-conformance or breach by any colleague or third-party will be subject to investigation and may lead to disciplinary actions, up to and including termination of employment/contract.

Glossary

Acronym	Meaning
SLT	Senior Leadership Team
ISMS	Information Security Management System
ISF	Information Security Forum

Annex A

Compliance References

Standard	Control	Control Title
ISO/IEC 27001:2013	4	Context of the organisation
ISO/IEC 27001:2013	5	Leadership
ISO/IEC 27001:2013	6.1.1	General
ISO/IEC 27001:2013	6.2	Information security objectives & planning to achieve them
ISO/IEC 27001:2013	7.1	Resources
ISO/IEC 27001:2013	7.2	Competence
ISO/IEC 27001:2013	7.3	Awareness
ISO/IEC 27001:2013	7.4	Communication
ISO/IEC 27001:2013	10	Improvement
ISO/IEC 27001:2013	A.5.1.1	Policies for information security
ISO/IEC 27001:2013	A.6.1.1	Information security roles and responsibilities
ISO/IEC 27001:2013	A.6.1.5	Information security in project management
ISO/IEC 27001:2013	A.7.2.1	Management responsibilities
ISO/IEC 27001:2013	A.7.2.2	Information security awareness, education, and training
GDPR	Art. 5	Principles relating to processing of personal data
GDPR	Art. 32	Security of processing

Version Control

This is a controlled document produced by Acceleraate Ltd. The control and release of this document is the responsibility of the document owner. This includes any amendment that may be required. This document is ©Acceleraate Ltd, unless otherwise stated.

#	Change	Date	Author	Approved
V1.1	Document issued	01.03.23	Ben Jemison	01.03.23
V1.2	Reviewed without changes	01.03.24	Ben Jemison	01.03.24

Document Classification

Public