Information Security Policy

Navitas Limited
ACN 109 613 309

Document

Document Name	Information Security Policy
Responsibility	Global Head of Information Security
Initial Issue Date	01/03/2018

Version Control

Date	Version No.	Summary of Changes	Reviewer Name and Department/Office
01/03/2018	1.0	Initial Release	G. Ryan – Navitas IT
08/05/2018	2.0	Review and Update	Navitas IT
06/05/2019	3.0	Review and Update	Navitas IT
08/05/2020	4.0	Review and Update	Navitas IT
03/05/2021	5.0	Review and Update	Navitas IT

Related Documents

Name	Location

Contents

1 Purpose and Scope

1.1 Introduction

This Information Security Policy ("**Policy**") sets out the global approach of Navitas Limited and its affiliated group companies (together the "**Company**") relating to Information Security.

1.2 Purpose

The purpose of this Policy is to outline the Company's statement of intent on how the Company provides Information Security and to reassure all parties involved with the Company that their information is protected and secured.

1.3 Scope

This Policy has been prepared in accordance with the Company's legislative requirements and principles. The Policy applies to all Company systems, information and users (meaning permanent, part-time, contractors, volunteers, interns and third parties).

2 Policy Statement

2.1 Management Commitment to Information Security: The Company Leadership Team, shall actively support Information Security within the Company with clear direction, demonstrated commitment and explicit acknowledgement of Information Security responsibilities.

2.2 Security Assessments and Authorisation: The Company shall periodically assess systems to determine if Information Security controls are operating effectively and monitor on an ongoing basis to ensure the continued effectiveness of those controls.

2.3 Planning: The Company shall develop, document, implement, and periodically update measures to protect its critical systems.

2.4 Program Management: The Company shall implement Information Security program management controls to provide a foundation for the Company's' Information Security Management System.

2.5 Risk Assessment: The Company shall periodically assess the risk to operations, assets, and information, resulting from the operation of systems and the associated processing, storage, or transmission of information.

2.6 System and Service Acquisition: The Company shall allocate sufficient resources to adequately protect systems by employing a System Development Life Cycle (SDLC) process that incorporate Information Security considerations.

2.7 Awareness and Training: The Company shall ensure that users are made aware of the Information Security risks associated with their roles and that users understand their obligations and the applicable laws, policies, standards, and procedures related to the security of systems and information.

2.8 Contingency Planning: The Company shall establish, implement and maintain plans for the continuity of operations in emergency situations to ensure the availability of critical information resources.

2.9 Incident Response: The Company shall establish an actionable Information Security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

2.10 Media Protection: The Company shall protect system media, both hardcopy and digital, by limiting access to authorized users and sanitizing or destroying media so that unauthorized information recovery is technically infeasible.

2.11 Personnel Security: The Company shall ensure that published rules of behavior are followed by users and employ a method of formal sanctions for personnel who fail to comply with Information Security policies and standards.

2.12 Physical and Environmental Protection: The Company shall implement physical access controls to limit access to systems, equipment, and the respective operating environments to authorized individuals. The Company shall provide appropriate environmental controls in facilities containing systems.

2.13 Access Control: The Company shall implement logical access controls to limit access to systems and processes to authorized users.

2.14 Audit and Accountability: The Company shall create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity by ensuring that the actions of individual users and systems can be uniquely traced.

2.15 Configuration Management: The Company shall maintain accurate inventories of its systems and enforce security configuration settings for information technology products employed in support of the Company's business operations.

2.16 Identification and Authentication: The Company shall implement mechanisms are employed to properly identify system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices.

2.17 Maintenance: The Company shall perform periodic and timely maintenance on systems, so that Company assets are protected from the latest threats.

2.18 System and Communication Protection: The Company shall employ industry-recognized leading practice principles that promote effective Information Security within systems and the network.

2.19 System and Information Integrity: The Company shall correct flaws in its systems in a timely manner and ensure mechanisms are in place to protect systems from malicious code.

3 Compliance

3.1 General

All users who have access to Company systems and information are required to read this policy.

3.2 Breaches

Breaches of policy compliance may result in disciplinary action being taken against the offender.

3.3 Relevant Legislation

The Company is a global organisation with the responsibility to maintain compliance with the laws within our host nations. All Company users are responsible for aiding the Company in identifying relevant legislation and for complying with all relevant legislation.

4 Responsibilities

Each of the positions involved in implementing and achieving policy objectives and carrying out procedures are shown here.

Responsibility	**Global Head of Information Security**	**Company IT Gov.**	**Company IT Leaders**	**Company Users**
Approver of Document	A			
Maintenance of Document		A		
Review of Document			C	C
Understanding of document			R	R

R = Responsible, A = Approve, S = Supporting, C = Consulting, I = Informed.

5 Definitions

Unless the contrary intention is expressed in this Policy, the following words (when used in this policy) have the meaning set out below:

Term	Meaning
Company	Means Navitas Limited and its affiliated group companies.
Systems	Encompasses applications, software, laptops, desktops, servers and networking equipment

6 Review

This Policy is tested and reviewed and any changes to the regulatory compliance requirements, legislation, regulation and guidelines. This review process aims to ensure alignment to appropriate strategic direction and continued relevance to the Company's current and planned operations.

7 Records Management

All records in relation to this document will be managed as follows:

Record type	Owner	Location	Retention	Disposal
Policy	Global Head of Information Security	Electronic	Permanent	N/A

8 Appendix A – Information Security Framework

To ensure a holistic approach to Information Security is applied across Navitas, a formal Information Security Framework has been developed. The Information Security Framework has been developed based on the globally recognised NIST framework. The NIST framework directly maps with other global frameworks. This has enabled the Navitas Information Security Framework to be further tailored to align with business objectives and requirements.