Physical and Environmental Security Policy

Navitas Limited
ACN 109 613 309

Document

Document Name	Physical and Environmental Security Policy
Responsibility	Global Head of Information Security
Initial Issue Date	22/03/2018

Version Control

Date	**Version No.**	**Summary of Changes**	**Reviewer Name and Department/Office**
22/03/2018	1.0	Initial Release	G. Ryan – Navitas IT
08/05/2018	2.0	Review and Update	Navitas IT

Related Documents

Name	**Location**
Information Security Policy	Intranet
IT Acceptable Use Policy	Intranet
Information Classification Policy	Intranet

Contents

1 Purpose and Scope

1.1 Introduction

This Physical and Environmental Security Policy ("**Policy**") sets out the global approach of Navitas Limited and its affiliated group companies (together the "**Company**") relating to the provision of a safe and secure work environment.

1.2 Purpose

The purpose of this Policy is to ensure that the appropriate measures are taken to keep Company information, facilities and people safe. It is designed to articulate the responsibilities and controls required to provision a safe and secure work environment.

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 and to all employees within the Company (meaning permanent, part-time, contractors, volunteer and interns)

2 Policy Statement

2.1 General

2.1.1 Physical access to the Company's sensitive information processing facilities is to be restricted to authorised personnel only.

2.1.2 Secure areas must be protected with a combination of access control devices and access logging equipment.

2.1.3 Physical access rights must be reviewed on a quarterly basis.

2.1.4 Physical access rights must be revoked at the end of the employees' final day of employment with the Company or completion of a third party engagement.

2.1.5 It is the responsibility of all employees to remain vigilant and request identified of any individual acting suspiciously or not recognized as a Company employee.

2.1.6 All employees are responsible for ensuring the security of access cards allocated for personal use. Employees will be held accountable for actions carried out through the use of personal access cards.

2.1.7 All employees must adhere to a clear desk policy at all times and store all documentation and removable media in line with the *Information Classification Policy*.

2.1.8 All employees must lock screens or log-off desktops / laptops when not being used.

2.1.9 The removal of all non-personally provisioned equipment without management authorisation is strictly prohibited.

2.1.10 All core communications equipment such as routers, switches, hubs, repeaters and patch panels must be located in a secure area with a locked entrance and accessed by authorised personnel only.

2.2 Physical Access Visitors

2.2.1 All visitors must report to the reception area and provide details as required, which will be recorded in a Visitors Register.

2.2.2 Visitors must be met by the employee they have come to meet or by a nominated representative.

2.2.3 Visitors will only be issued security passes where their stay is extended for one day. The receiving employee will be responsible for authorising the issuing of a pass and give dates and sign for pass.

2.2.4 Where a pass has been issued, the employee who authorised the pass will be responsible for retrieving the pass on completion of the visit.

2.2.5 Where possible, a meeting room should be used to meet with visitors to reduce the possibility of inadvertently exposing confidential information.

2.3 Environmental Controls

2.3.1 The following minimal environmental controls must be maintained for all information processing facilities:

- Environmental condition monitoring system with alert functionality activated and allocation of contact personnel.
- Air-conditioning units to maintain adequate systems operating temperature.
- Fire suppression system.
- Power supply redundancy in the event of power failure.
- Uninterruptible power supply to protect against power surges, spikes or brownouts.
- Raised flooring to protect against water damage.

2.3.2 Testing of environmental controls where practical must be conducted and results recorded on a minimum six monthly basis.

2.4 Guidelines for Working within Secure IT Areas

2.4.1 All third party activity or work must be approved by Group IT and supervised by a Company employee.

2.4.2 Vacant secure IT areas should be physically locked and periodically checked.

2.4.3 Recording equipment (e.g. cameras, videos, phones) should not be used in secure IT areas unless authorised by Group IT.

3 Compliance

3.1 General

All employees of the Company 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	CIO	Company IT Gov.	Company IT Leaders	Company Employees
Approver of Document	A			
Maintenance of Document		A		
Review of Document		A	C	C
Understanding of document	R	R	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 ACN 109 613 309 having its registered office at Level 8, Brookfield Place, Perth, 6000.
Website (where relevant)	Means the Company’s website where information is available to employees, shareholders and other interested persons or organisations.
Processing Facility	Means the location where server and supporting network infrastructure is stored.

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