

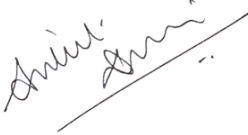
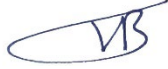





National Credit Guarantee Trustee Company Ltd

Information Security Policy

Doc. No. : NCGTC-ISMS-PL-01
Issue No. & Date : Ver 1.0 & 05-04-2023
Classification of Information : Internal and protected
Revision Status : Ver 1.0

	Name	Designation	Signature	Date
Prepared by	Kratikal Tech Pvt Ltd	Compliance Team		05-01-2023
Reviewed by (Internal)	Ajay Prajapati	Manager		20-01-2023
Reviewed by (External)	Ankit Desai	Information Security Consultant		10-03-2023
Approved by	Vijayraj Bhosale	CISO		13-03-2023

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

Revision Status

Revision	Date	Page No.	Clause No.	Brief Description of Revision
00	20-01-2023	All	All	The initial issue to comply with the requirements of ISO 27001:2022
01	13-03-2023	All	All	Minor changes done in the document.
01	05-04-2023	All	All	Policy document issued post approval from board dated 23-03-2023.

All rights reserved.

The information in this document is the property of NCGTC (National Credit Guarantee Trustee Company Ltd) and is exclusively prepared for NCGTC.

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of NCGTC.

Legal action may be taken against any infringement.

Errors and Omissions

In case of any errors or omissions are noted in this document, please report same to Chief Information Security Officer (CISO), NCGTC Ltd on email id CISO@ncgtc.in



	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

Table of Contents

TABLE OF CONTENTS	3
1. PURPOSE	4
2. SCOPE	4
3. ROLES & RESPONSIBILITIES	4
4. ABBREVIATIONS & DEFINITIONS	5
4.1 ABBREVIATIONS	5
4.2 DEFINITIONS	5
5. FORMS	5
6. INFORMATION SECURITY POLICY	6
6.1 INFORMATION SECURITY REQUIREMENTS	6
6.2 FRAMEWORK FOR SETTING OBJECTIVES.....	6
6.3 CONTINUAL IMPROVEMENT OF THE ISMS.....	7
6.4 INFORMATION SECURITY POLICY AREAS.....	8
TABLE 1: SET OF POLICY DOCUMENTS	8
6.5 APPLICATION OF INFORMATION SECURITY POLICY.....	13
7. REFERENCE DOCUMENT	13
8. ENFORCEMENT	14

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

1. Purpose

This document defines the Information Security Policy of NCGTC.

As a modern, forward-looking business, NCGTC recognizes at senior levels the need to ensure that its business operates smoothly and without interruption to benefit its customers and other stakeholders.

To provide such a level of continuous operation, NCGTC has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognized best practices.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements


NCGTC has decided to maintain full certification to ISO/IEC 27001 so that an independent third party, a Registered Certification Body (RCB) may validate the effective adoption of information security best practices.

2. Scope

This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties with access to NCGTC's systems.

3. Roles & Responsibilities

Roles	Responsibilities
CISO	<ul style="list-style-type: none"> • Approve all Mandatory Documents • Approval & Communication Authority.

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

4. Abbreviations & Definitions

4.1 Abbreviations


Abbreviations	Expansions
NCGTC	National Credit Guarantee Trustee Company Ltd
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission

4.2 Definitions

Terms	Definitions
NA	

5. Forms

Name of the Document	Form No.
NA	

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date


6. Information security policy

6.1 Information security requirements

- 6.1.1** A clear definition of the requirements for information security within NCGTC will be agreed upon and maintained with the internal business and cloud service customers so that all ISMS activity is focused on fulfilling those requirements. Statutory, regulatory, and contractual requirements will also be documented and input into the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.
- 6.1.2** A fundamental principle of the NCGTC's Information Security Management System is that the controls implemented are driven by business needs, which will be regularly communicated to all staff through team meetings and briefing documents.

6.2 Framework for setting objectives

- 6.2.1** A regular cycle will be used to set objectives for information security to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.
- 6.2.2** Information security objectives will be documented for an agreed period, with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.
- 6.2.3** Per ISO/IEC 27001, the reference controls detailed in Annex A of the standard will be adopted where appropriate by NCGTC. These will be reviewed regularly in light of the outcome of risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded, please see the Statement of Applicability.


	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

6.2.4 Adopting this code of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

6.3 Continual Improvement of the ISMS

NCGTC 's policy regarding continual improvement is to:

- 6.3.1** Continually improve the effectiveness of the ISMS
- 6.3.2** Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards.
- 6.3.3** Achieve ISO/IEC 27001 certification and maintain it on an ongoing basis
- 6.3.4** Increase the level of proactivity (and the stakeholder perception of proactivity) about information security.
- 6.3.5** Make information security processes and controls more measurable to provide a sound basis for informed decisions.
- 6.3.6** Review relevant metrics on an annual basis to assess whether it is appropriate to change them based on collected historical data.
- 6.3.7** Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers.
- 6.3.8** Review ideas for improvement at regular management meetings to prioritize and assess timescales and benefits.
- 6.3.9** Ideas for improvements may be obtained from any source, including employees, customers, suppliers, IT staff, risk assessments, and service reports. Once identified, they will be recorded and evaluated as part of management reviews.


	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

6.4 Information Security Policy Areas


- 6.4.1** NCGTC defines policy in a wide variety of information security-related areas described in detail in a comprehensive set of policy documentation accompanying this overarching information security policy.
- 6.4.2** Each of these policies is defined and agreed upon by one or more people with competence in the relevant area. Once formally approved, it is communicated to an appropriate audience, both within and external to the organization.
- 6.4.3** The table below shows the individual policies within the documentation set and summarizes each policy's content and the target audience of interested parties.

Table 1: Set of Policy Documents


POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security, and monitoring and prohibited Internet service uses cases.	Users of the Internet service
Cloud Computing Policy	Due diligence, signup, setup, management , and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets, and smartphones, whether provided by the organization or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date


POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement, e.g., physical security, insurance, and equipment	Management and employees involved in setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities, and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security, and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring	Employees responsible for protecting the organization's infrastructure from malware

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
	and alerts, technical reviews, and malware incident management.	
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing, and protection of storage media	Employees responsible for designing and implementing backup regimes
Logging and Monitoring Policy	Settings for event collection, protection and review	Employees responsible for protecting the organization's infrastructure from attacks
Software Policy	Purchasing software, software registration, installation and removal, in-house software development, and cloud software use.	Employees responsible for purchasing, installation, development, and management of cloud
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening, and awareness training.	Employees responsible for protecting the organization's infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks, and remote access; network security management, including roles and	Employees responsible for designing, implementing, and managing networks


	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
	responsibilities, logging and monitoring, and changes.	
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring electronic messaging facilities, and use of email.	Users of electronic messaging facilities
Secure Development Policy	Business requirements specification, system design, development and testing, and outsourced software development.	Employees responsible for designing, managing, and writing code for bespoke software developments
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes, and end of the contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans, and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties , and software license compliance.	All employees
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media	Employees responsible for the creation and management of records

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
	selection, record retrieval, destruction, and review.	
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions, and requirements.	Employees responsible for designing and managing systems using personal data
Clear Desk and Clear Screen Policy	Security of information shown on screens printed out and held on removable media.	All employees
Social Media Policy	Guidelines for how social media should be used when representing the organization and discussing issues relevant to the organization.	All employees
HR Security Policy	Recruitment, employment contracts, policy compliance, disciplinary process, termination	All employees
Acceptable Use Policy	Employee commitment to organizational information security policies	All employees
Asset Management Policy	This document sets out the rules for managing assets from an information security perspective.	All employees

Table 1: Set of policy documents

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date


6.5 Application of Information Security Policy

6.5.1 The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of NCGTC and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action under the organization's Employee Disciplinary Process.

6.5.2 Questions regarding any NCGTC policy should be addressed to the employee's immediate line manager.

7. Reference Document


- Risk Assessment and Treatment Process
- Statement of Applicability
- Supplier Information Security Evaluation Process
- Internet Acceptable Usage Policy
- Cloud Computing Policy
- Mobile Device Policy
- Teleworking Policy
- Access Control Policy
- User Access Management Process
- Cryptographic Policy
- Physical Security Policy
- Anti-Malware Policy
- Backup Policy
- Logging and Monitoring Policy
- Software Policy
- Technical Vulnerability Management Policy
- Network Security Policy

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

- Electronic Messaging Policy
- Secure Development Policy
- Information Security Policy for Supplier Relationships
- Availability Management Policy
- IP and Copyright Compliance Policy
- Records Retention and Protection Policy
- Privacy and Personal Data Protection Policy
- Clear Desk and Clear Screen Policy
- Social Media Policy
- HR Security Policy

8. Enforcement

All employees, user departments, vendors, and third parties shall follow the policy; violating this could lead to contract termination or financial penalties.

	Information Security Policy				
	Doc. No.	<i>NCGTC-ISMS-PL-01</i>	Classification of Information	<i>Internal and protected</i>	Rev. Version & Date

Document Note

This document of NCGTC conforms to the Onsite Team of the National Credit Guarantee Trustee Company Ltd. It is stored in the Process Repository, accessible through authorized IDs connected to LAN. Printed or other electronic copies are for information only.

The user is responsible for assuring that they always use the currently valid version at the address mentioned above.

This document ends here.