Â

INFORMATION SECURITY POLICY

COFORGE LIMITED

NOTICES

Document Name: Information Security Policy

Version 5.0

Issued By: MR

Date: 13th May 2022

Approved By: Dr. Jitendra Mohan Bhardwaj (CISO)

Classification: Internal/Protected

CONTENTS

DISTRIBUTION AND CONTROL OF THE DOCUMENT

All copies of the document will be issued, controlled and distributed Representative.

Controlled Copy Holders.....

1. Intranet Server.....
2. Corporate Internet Server https://iengage.coforge.com.....

The document is controlled by ensuring that all revisions to be made to th into the Revision List page. The ISMS release note for each release is appro

It is also ensured that obsolete pages of the document are identified and re

---

05 Information Security Policy

Purpose

The purpose of this policy is to manage Information Security within appropriate security controls to protect its information processing facilities.

Scope

This Information Security Management System (ISMS) is an apex documer to all its facilities located at

- Tech Zone, Plot# 2 & 2A, Yamuna Expressway, Greater Noida, Uttar Pra
- Plot # 223-224, Udyog Vihar, Phase 1, Gurgaon, Haryana â€“ 122002, I
- Plot No-H7 Sector 63, Noida â€“ 201301, U.P., India
- Ecospace Business Park, 3B -501, 5th Floor, Kolkata â€“ 700091, India
- No.31/2, Roopena Agrahara, Begur Hobli, Hosur Main Road, Bangalore
- 4th Floor, Tower B, Marwah Centre, Krishnalal Marwah Marg, Off Saki Mumbai â€“ 400072, India
- Block B,6th Floor Q City, SR No. 109, 110, 111/12, Nanakramguda Mandal, Ranga Reddy District, Hyderabad 500032
- 2nd Floor, 47 Mark Lane, London - EC3R 7QQ, United Kingdom, U.K.
- Bockenheimer LandstraÃŸe 51-53, 60325 Frankfurt am Main, Germany
- Lina-Ammon-Strasse 19b, 90741 NÃ¼rnberg, Germany
- 502 Carnegla Center Drive, Suite # 301 Princeton, New Jersey, 08540 U
- Bureau 707, 7th floor, 135 Paseo de la, Castellana, 28045, Madrid, Spa

It applies to:

All users of the Information Assets including, but not limited to empl contractoÂrs, vendors, customers and business partners.

All Information Systems (IS) environments operated by Coforge in its fac environmentâ€□ defines the total environment and includes, but documentation, physical, environmental and logical controls, hardware, s for the following business processes:

- IT Services
- Information Technology Support
- Human Resources
- Administration
- Projects

Responsibility

The responsibility of ensuring adherence to this policy lies with all Cofo within the scope of the ISMS. The CISO is responsible for coordinati monitoring, controlling, reviewing and improving the ISMS under the dire Management Committee.

5.1 Management Directions for Information Security

To provide management direction and support for information security business requirements, and relevant laws and regulations.

5.1.1 Policies for Information Security

Coforge is committed to protecting the confidentiality, integrity, and availa Assets, and provide the same commitment to the information assets customers.

Coforge shall strive to secure information by:

- Maintaining an effective Information Security Management System.

- Deploying most appropriate technology and infrastructure, based on
- Creating and maintaining a security conscious culture within Coforge
- Continually monitoring and improving the effectiveness of the Management System.

5.1.1.1 Organization of Information Security

The organization shall establish the Management Information Security F management forum comprising of the Heads of the various Business Functions with the following objective:

- Demonstrate management commitment and provide visible support initiatives within the organization.
- Provide direction and guidelines for the establishment and implemer policies required.
- Establish the roles and allocate responsibilities for information securit
- Approve the risk assessment methodology and the criteria for accept
- Conduct management reviews of the ISMS.
- Establish the Information Security Team (IST) with the role to in security implementation at planned intervals.

The organization shall establish policies and processes for executing c disclosure agreements with its employees reflecting the need for the prote assets.

The organization shall maintain contact with appropriate authorities and sp order to ensure prompt and effective coordination and assistance during em

The organization shall identify, and address risks related to access and exp assets, by external parties, including customers by covering relevant s agreements / contracts and non-disclosure agreements.

5.1.1.2 Human Resources Security

The security roles and responsibilities of all employees including temporar third-party service providers requiring access to Coforge facilities, infor assets shall be defined and documented.

Screening and background checks shall be performed as a part of the re recruiting personnel for all roles having access to Coforge information asset

All employees (including employees of third party/outsourced agency, not contract), having access to Coforge information will have to sign a confi part of a formal contract with Coforge. The contract shall also clearly conditions of employment.

All employees will have to mandatorily appear for the ISMS training o subsequently appear for the ISMS certification test at the time of joining, every year thereafter. Login ID shall be created for new joiners post succ ISMS test. For any exception to this, approval from CISO shall be sought.

Security training and awareness programmes shall be conducted as a part at the time of audit (NIP) for new personnel. NIP is followed by e NIP, and at periodic intervals, to keep all personnel updated with the prevalent infor in the organization.

All employees including temporary staff and contractors, and third-party se subject to the disciplinary process of the organization for any violations of Policies and Procedures. A formal Disciplinary Action Policy shall be formul across the organisation.

Policies, procedures for termination of employment, or change of employm and implemented, and responsibilities assigned.

A process shall be implemented to ensure that all employees including tem
and third-party service providers return all of the organizationâ€™ assets i
termination, or change of their employment, contract, or agreement.

Access rights of all employees including temporary staff, contractors
providers to information and information processing facilities shall be
termination, or, in case of change of their employment, contract or agreeme

5.1.1.3 Asset Management

All Information assets will be accounted for in an Information Asset Registe
maintained by the asset owners. Periodic risk assessment shall be performe
plans shall be documented in the Information Asset/Risk Register.

The Asset Owners shall ensure that the information assets are protected in
commensurate to their classification and valuation. Information Asset Owne
for updating the information assets/Risk register on a regular basis, or at th
changes in the technology or infrastructure in the area of their responsibilit
will be labelled, and handled as per their classification.

Policies and rules shall be implemented for the acceptable use of informatio
with the applications, information systems and network services.

The Information Security Team (IST) shall review the asset register and the
periodic internal audits.

5.1.1.4 Access Control

IST shall be responsible for safeguarding information and information p
various business, and environmental threats, with the assistance of HR, A
Operations Team. IST will facilitate the development and implementa
protecting information assets from unauthorized modification, disclosure or

The access rights will be granted by the respective Information Asset Owr
are commensurate to business requirements. Project/Function shall m
access to information and information-processing facilities are controlled a
to-know basis, and commensurate to business and security requirements.

The procedures for granting access to information assets will be based on
impact resulting from the loss of its confidentiality, integrity and availability

5.1.1.5 Cryptography

To ensure proper and effective use of cryptography to protect the con
and/or integrity of information.

5.1.1.6 Physical and Environmental Security

Physical security perimeters shall be established to protect the facilit
unauthorized access. Additionally, different areas of the facility shall be
based on the criticality and sensitivity of the information assets, or informa
located within those areas, and access control mechanisms implemented
the facility. The following zoning scheme shall be followed in all the facilities

- Restricted zone
- Internal zone
- Public zone

All information processing facilities will be housed in secure areas and shall
protected from damage by physical and environmental threats.

Equipment shall be protected from power and other utilities failure. Critical
equipment shall be correctly maintained to ensure continued availability.

Sensitive data and licensed software in systems and storage media shall be / degaussed prior to disposal or re-use.

5.1.1.7 Operations Security

Information Asset Owners shall ensure that the management and op processing facilities is controlled and monitored, to minimize the risk due to safeguard the availability and integrity of the information or assets.

Operating procedures required for ensuring the management and op processing facilities shall be documented, maintained and used.

Changes to any operational information processing facilities, systems, and shall be controlled through the use of a formal change management pro changes are authorized.

Duties and areas of responsibility in critical and sensitive roles shall be seg of unauthorized access, or changes to any operational systems and IT infras

The organizationâ€™s business communication facilities shall be used for of

5.1.1.8 Communications Security

The IT Operations team shall ensure the protection of information in netw information processing facilities from logical, physical and environmental th

5.1.1.9 Systems Acquisition, Development and Maintenance

Information Asset Owners are responsible for identifying security contro information systems of Coforge. IST shall validate the same to ensure commensurate to the classification of the information assets. The impleme maintenance of information systems at Coforge shall be carried out b requirements identified by the Information Asset Owners.

5.1.1.10 Supplier Relationships

To ensure protection of the organizationâ€™s assets that are accessible controls shall be established by respective functions. The IST shall periodically to ensure that Coforge information assets are protected classification. Non-Disclosure Agreements and sharing of the relevant secu suppliers shall be ensured.

5.1.1.11 Information Security Incident Management

All security incidents shall be reported to IST information security team, or authority for the purpose.
All information security incidents shall be handled in a manner commensura and valuation of the information asset and shall be properly documented.

5.1.1.12 Information Security Aspects of Business Continuity Manag

All Information Asset Owners shall develop and maintain business co respective functions, programs and projects, with assistance from t interruptions to business activities and, to protect critical business proce major failures or disasters. These business continuity plans will be tested basis (as per customer requirement). Any exception shall be documente justification along with Delivery Head and Customer approval.

5.1.1.13 Compliance

The Business Unit and Function Heads shall ensure compliance with inforı procedures and applicable laws, and regulations with respect to business employees, contractors, and third-party suppliers shall adhere to the purpose of maintaining the compliance.

5.1.2 Review of the Policies for Information Security

CISO is the owner of the Information Security Policy document, and custodian.

CISO and the IST are primarily responsible for the effective implementation Policies. The policy shall be reviewed for effectiveness once in a year, or change in Coforgeâ€™s operational or technical environment.

Localisation of Operating Procedures

Based upon the size, technology and complexity of operations in a Co procedures may be tailored subject to approval by the MISF.

Exception

Management at its discretion may decide to waive some or all of these rec to the business requirements and associated risks. Such waivers shall be d Steering Committee.

Revision List

Document Name: Information Security Policy

DATE	PARAGRAPH/ SECTION NO.	NATURE OF AMENDMENT	NEW VERSION
02/05/2022	05 Information Security Policy	HYD location added in Scope	5.0
10/06/2021	05 Information Security Policy	Reviewed and no changes has been done.	4.0
04/09/2020	05 Information Security Policy	Changes in line with company's rebranding to Coforge Limited.	4.0
03/03/2020	05 Information Security Policy	Removed one location from Scope, NIP is followed by E-NIP in awareness methodology	3.4
22/02/2019	05 Information Security Policy	Spain office address has changed to C/MÃ©ndez Ã□lvaro 9, 2nd floor, 28045, Madrid, Spain	3.3
27/01/2018	05 Information Security Policy	Included Overseas Delivery Centres of UK, US, Germany and Spain	3.2
27/02/2017	05 Information Security Policy	Mumbai location included	3.1
21/03/2016	05 Information Security Policy	Reviewed and no changes made.	3.0

15/03/2015	05 Information Security Policy	Mapping of document inline to new ISO 27001:2013 standard.	3.0
22/10/2014	05 Security Policy	Reviewed but no changes made in the Security Policy.	2.1
26/08/2013	05 Security Policy	Reviewed but no changes made in the Security Policy.	2.1
15/04/2013	05 Security Policy	• Process for ISMS internal certification for new joiners identified under section 5.1.1.3 Human Resource Security • Responsibilities for creating and distributing security policy explicitly defined under section 5.1.2 Review of Information Security Policy	2.1
24/07/2012	05 Security Policy	1. Classification of the Security Policy changed from "Internal" to "Internal/ Restricted" 2. ISMS scope modified to include Mumbai facility 3. Revision History updated to capture history of changes made in the policy	2.0
25/04/2012	05 Security Policy	ISMS scope modified to exclude Mumbai facility	1.9
31/08/2011	05 Security Policy	ISMS scope modified to include Greater Noida facility	1.8
30/03/2010	05 Security Policy	Included a new table with approving, reviewing and releasing authorities along with custodian under sec. 5.1.3 - Review and evaluation.	1.7
24/03/2009	05 Security Policy	ISMS scope modified to exclude H9 (Colosseum) and include H7, Sector 63, Noida facility.	1.6

05/09/2008	05 Security Policy	Security Policy is classified as an Internal document	1.5
25/07/2008	05 Security Policy	1) ISMS scope modified to exclude Kalka Ji, New Delhi 2) Updated section 5.1.1.3 Human resources security to synchronize with 8.1.2: Screening Old contents: • Delivery Head level and above • Members of HR team • Members of ICO and DLA teams • All personnel recruited for BFSI projects	1.4
20/05/2008	05 Security Policy	Reference of Athena removed to make it applicable to all locations Modified the ISMS scope to include different locations	1.3
15/03/2007	05 Security Policy	Aligned with ISO 27001 standard control objectives	1.2
31/01/2006	03 Security Policy	Changed the scope to cover the whole organisation	1.1