IR 123 Acceptable Use Policy

Coforge

IR 123 Acceptable Use Policy

Coforge

Please direct all Enquiries with Respect to this Document to:

Name	Designation	Contact Details
Information Security Team	Security Team	AllatIST@coforge.com

Terms and Abbreviations

ABBREVIATION	TERM
CISO	Chief Information Security Officer
CFO	Chief Financial Officer
DLP	Data Leakage Prevention
SRS	Software Requirement Specification
HLD	High Level Diagram
LLD	Low Level Diagram
SOW	Scope / Schedule of Work
WFH	Work From Home
PI	Personal Information
SPI	Sensitive Personal Information
PED	Portable Electronic Device
VPN	Virtual Private Network
USB	Universal Serial Bus

Table of Contents

IR 123 Acceptable Use Policy

Coforge

Purpose

The purpose of the Coforge Acceptable Use Policy is to establish acceptable practices regarding the use of Coforge Information Resources to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Scope

The Coforge Acceptable Use Policy applies to any individual, entity, or process that interacts with any Coforge Information Resource.

Acceptable Use

- Employees are responsible for complying with Coforge policies when using Coforge information resources and/or on Organization time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Team / Supervisor.
- Personnel must promptly report harmful events or policy violations involving Coforge assets or information to their manager or a member of the Information Security Team.
- Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Coforge Information Resources.
    - Data incident: any potential loss, theft, or compromise of Coforge information.
    - Unauthorized access incident: any potential unauthorized access to a Coforge Information Resource.
    - Facility security incident: any damage or potentially unauthorized access to a Coforge owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other Coforge policies, standards, or procedures

Computing and Network Facilities

The computing and networking facilities include all computing platforms, including local area networks, wide area networks, systems and applications used in Coforge.

Conditions of use

- Appropriate and reasonable use of the computing and networking facilities is defined as use that is consistent with objectives of the Company and with the specific objectives of the project or role for which such use was authorized. Coforge reserves the right to limit, restrict access to them.
- All persons using the computing and networking facilities shall be responsible for the appropriate use of the facilities provided as specified in the “Code of Practice" section of this document.
- IT Operations shall implement Windows Bit locker Encryption on all drives of Coforge laptops. Users should ensure that the bit locker encryption is enabled on all the drives containing critical, personally identifiable,

and confidential data.

- The company recognizes the need to protect the confidentiality of information and material furnished by clients or staff, and all computing personnel should protect the confidentiality of such information and material.
- The Company reserves the right to restrict or limit permanently, any user's usage of the computing and networking facilities with or without notice to the user in order to protect the integrity of the computing and networking facilities against unauthorized or improper use, and to protect other users.
- The Company, through authorized individuals, reserves the right to periodically check and monitor and take any action to protect computing and networking facilities from misuse.

An action will be deemed as misuse if the user is:

- Responsible for wilful physical damage to any of the computing and networking facilities.
- In possession of confidential information obtained improperly.
- Responsible for wilful destruction of information including official mails.
- Responsible for deliberate interruption of normal services provided by the computing facilities.
- Responsible for the infringement of any copyright, licensing, violation of condition for use or any other agreements.
- Using, gaining, or attempting to gain unauthorized access to accounts and passwords.
- Gaining or attempting to gain access to restricted areas without the authorization.

Code of Practice for Use

Objectionable Material

Coforge' s computing and networking facilities must not be used for transmission, obtaining possession, demonstration, and advertisement.

Or

Requesting transmission of objectionable material knowing it to be objectionable material.

The material may include, but is not limited to:

- Material meant for entertainment.
- Pornography Material or an article that describes or depicts, in a manner that is likely to cause offense to reasonable adults.
- An article that promotes crime or violence or incites or instructs in matters of crime or violence.
- An article that may disturb communal harmony.

Use of Sensitive System Tools and Utilities

Unless authorized, use of sensitive system tools and utilities such as password cracking tools, network sniffers, etc. are prohibited.

Harassment

Company policy prohibits all forms of harassment. Computing and networking facilities are not to be used to defame, insult, or harass any other person. The following, not limited to constitute examples of harassment:

- Intentionally using the facilities to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials, or threats of physical harm to the recipient, or the recipient's family.
- Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
- Intentionally using the computer to disrupt or damage work done by colleagues.
- Intentionally using the computer to invade the privacy, academic or otherwise, of another person, or the threatened invasion of the privacy of another person.

Use of Desktop/Laptop Systems

Users are responsible for the security and integrity of Coforge's information stored on their desktop/laptop system. Users should avoid storing passwords or other information that can be used to gain access to computing resources in a manner that could be easily accessed by unauthorized persons.

All end user systems (laptops and desktops) shall have Data Leak Prevention (DLP) and Content Filtering agents deployed to safeguard organizational information. IT Team Support shall ensure deployment and monitoring for violations. Exemptions shall need to be approved by Delivery Heads/ CFO / CISO.

Network Login Account

- Company provides a Login ID and password to every individual user to get access to the network resources.
- You must not share your account with family, friends, or any other person.
- It is recommended that you change your password every 60 days, or earlier.
- You may not use the account of any other person. If you inadvertently gain such access to any unauthorized information, you should report it as a security incident immediately.
- In certain circumstances, you may have to share an account with others where shared duties apply. This would need specific authorization by the Information Asset Owner. In such cases, all sharers are jointly responsible for the account but may not share with others outside the group.

Electronic Mail Facilities

Electronic mail is critical to the normal conduct of business. The conditions of use cover all electronic mail systems owned by Coforge, or any other electronic mail systems used from within Coforge network, or while acting in an official capacity.

Conditions of use

1. All employees will have an e-mail account. The e-mail system will provide a single externally accessible e-mail address for employees. The address will not contain the name of internal systems or groups.
2. Appropriate and reasonable use of the e-mail facilities is defined as use that is consistent with objectives of the Company and with the specific objectives of the project or role for which such use was authorized. Electronic mail and communications facilities provided by Coforge are for official communication. Limited personal use is acceptable if it does not hurt the interests of the company. Coforge reserves the right to limit, restrict or extend access to them.
3. All persons using the e-mail facilities shall be responsible for the appropriate use of the facilities provided as specified in the "Code of Practice" section of this document.
4. The company recognizes the need to protect the confidentiality of information and material furnished by clients, suppliers, or team Coforge, and all users should protect the confidentiality of such information and material. The company takes safeguard measures to protect information from losses within the Coforge's e-mail facilities. The user must also take all reasonable measures to further safeguard against any loss of information within the Coforge's e-mail facilities under his/her control.
5. Users of the e-mail facilities must recognize that when they cease to be formally associated with the company, their information may be removed from Coforge's e-mail systems without notice.
6. The Company reserves the right to limit permanently or restrict any user's usage of the e-mail facilities with or without notice to the user to protect the integrity of the e-mail facilities against unauthorized or improper use, and to protect other users.
7. The Company, through authorized individuals, reserves the right to periodically check and monitor and take any action to protect e-mail facilities from misuse.
8. E-mails of India stakeholders and staff of Band 4 and above shall be covered by Legal Hold functionality available in Office 365.

An action will be deemed as misuse if the user is:

- Responsible for wilful physical damage to any of the e-mail facilities.
- In possession of confidential information obtained improperly. This includes transmission of classified documents to any private email account.
- Responsible for wilful destruction of information and e-mails.
- Responsible for deliberate interruption of normal services provided by the e-mail facilities.
- Gaining or attempting to gain unauthorized access to accounts and passwords.

Code of Practice for Use

- Use of COMPANY e-mail to participate in chain letters is forbidden.
- The use of COMPANY e-mail in any way to facilitate the conduct of a private, commercial purpose, gains, free offers, or schemes is forbidden.
- If the COMPANY provides access to electronic mail to external users such as consultants, temporary employees, or partners, they must read and adhere to Standards and Guidelines for use of e-mail. The usage must be strictly for services to Coforge.
- Confidential or company proprietary information shall not be sent to private or non-Coforge email account.
- All electronic messages created and stored on Coforge's computers or networks are property of the company and may not be considered private.
- Users must not allow anyone else to send e-mail using their accounts. This includes their supervisors, secretaries, assistants, and any other subordinates.
- Incoming messages will be scanned for viruses and other malware content.
- As Coforge's networks and computers are the property of the company, Coforge retains the right to allow authorized Coforge staff to monitor and examine the information stored within.
- It is recommended that personal confidential material not be stored on or sent through Coforge's equipment unless it is a clear business requirement and does not violate any regulatory requirement.
- Users must ensure the integrity of their password and abide by guidelines on selection and security of their password.
- As far as possible, Sensitive confidential material should be sent through the electronic mail system after encryption or password protection.
- Transmission of Sensitive (Contract, Flow Chart, Network Diagram, IP Scheme, SOW, Estimation, Financial Data, Customer Data, Software Requirement Specification (SRS), HLD, LLD, any kind of Source Code, Project Plan etc.) documents to private email accounts is prohibited.
- Users should refrain from any sort of electronic communication activity that puts the Company at risk or a lawsuit or financial loss.
- Users e-mailing to any person(s) outside of Coforge should clearly identify the user by full name and Designation. Additionally, the user's official and personal telephone number should also be provided.
- Subscription of any electronic communication distribution lists (e.g., subscriptions to stock market updates, movie updates, weather updates that are received regularly) that are not relevant to user's assigned duties is strictly prohibited.
- Email facility should not be used to support, oppose, or put opinions about political issues without prior approval from the management.

Communication Using Office 365

Office 365 services are available for staff to conduct and communicate organization business. Incidental personal use of email or other tools is allowed with the understanding that the primary use should be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

Office 365 applications include email access, Microsoft teams, Yammer, and One Drive and One note for Business.

For users having domain joined laptops, Office 365 applications (email, one note, one drive for Business) cannot be accessed through personal desktop/laptop unless the device is registered under Coforge AD Domain and has windows 10 Professional/Enterprise edition installed.

As a rule, user in the Intune group can access Coforge Office 365 services from their personal mobile devices by using the relevant Microsoft applications only after enabling full-disk encryption (The encryption algorithm used depends on the device operating system), on their mobile devices and enrolling their mobile device through Intune (Company Portal Mobile Application).

Email on the mobile can be accessed only through outlook client and cannot be accessed through any mobile native client.

One drive for business can only be accessed through One Drive client and not through any web browser. Share Point is not included as part of office 365 applications.

Unacceptable uses of the office 365 applications include, but are not limited to, the following:

- Storage and transmission of materials that infringes on the copyright laws, including intellectual property rights.
- Storage of data and using the office 365 applications for conducting personal business.
- Storage of data and sending / forwarding e-mails that are abusive, defamatory, derogatory, threatening, offensive or contains obscene or indecent materials.
- Unauthorized transmission of confidential material concerning business activities.
- Creation or transmission of anonymous email messages or using someone else's identity/password.
- Creation or transmission of material which is designed or likely to cause annoyance, harassment, inconvenience, or needless anxiety to the recipients.
- Provide unauthorized use of organization Office 365 facilities and skype for business to third party.
- Storage and transmission of unsolicited commercial or advertising material, chain letters, spam mail or other junk-mail of any kind.
- Storage of data and email activities that can corrupt other users' information or cause network interruptions, such as unauthorized broadcasting or mass mailings.

Internet Access Facilities

Connectivity and services offered via the Internet introduce new opportunities and new risks. In response to the risks, this document describes Coforge's policy regarding Internet security. It applies to all who use the Internet with Coforge's computing and networking resources.

The Internet is considered a valuable company asset. Users are encouraged to make use of the Internet and explore its uses. With such open internet access, employees must maintain a diligent and professional working environment. Employees are authorized incidental use which does not interfere with the performance or professional duties, is of reasonable duration and frequency, serves a legitimate company interest, such as enhancing professional interests or education, and does not overburden the system or cause any additional expense to the company.

Access to certain websites such as hacking, pornography, sports, and entertainment has been blocked. Users should not attempt to access such sites.

Conditions of use

- At any time and without prior notice, the company reserves the right to examine e-mail, Internet usage, personal file directories, and other information stored on Coforge's computers. This examination assures compliance with internal policies, promotes purposeful usage, and assists in management of Coforge's information systems.
- Access to the Internet from a company-owned home computer or through company-owned connections must adhere to all same policies that apply to use from within company facilities.
- A firewall has been placed between Coforge's computing & networking facilities and the Internet to protect our systems. Employees must not circumvent the firewall by using modems or any other means to obtain direct connectivity to the Internet.

Code of Practice for Use

- Use of the Internet should primarily be for business purposes only.
- Posting on the Internet any information or statements regarding Coforge without prior approval from the management is prohibited.
- Users should not interfere with the performance of professional duties.
- Users should not overburden the system or cause any additional expense to the company.
- Users should not access any obscene or pornographic sites and should not access or use information that would be considered harassing.
- Users should not engage in any Internet activity that puts the Company at risk of a lawsuit or financial loss.
- Posting non-business-related comments or statements on any web page or sending such messages over the Internet is prohibited.
- Entering non-business-related Internet chat rooms/channels on the Coforge corporate network is prohibited.
- Users should not subscribe to any services that broadcast material via the Internet. This includes listening to music or radio stations or receiving news and/or stock information via the Internet.
- Users should not use any publicly available material on internet in a manner that violates the Copyrights or trademark.
- All users who require access to Internet services must do so by using COMPANY-approved software and Internet Proxies.
- Users are not permitted to download and upload any software from the Internet unless authorized by their supervisors. All such requirements should be forwarded to the supervisor for authorization. Supervisors should verify licensing requirements and intended use before authorizing such downloading and forward the request to IT Team. IT team should ensure compliance of Intellectual Property Rights and screen the malicious content prior to installation.
- Users are strictly not permitted to use software "crack" files and license key generators to avoid IPR Infringement issues.
- Users should not misrepresent the source of anything they post or upload or impersonate another individual or entity, such as with "spoofing".

Work From Home Guidelines

- Adhere to all policies and procedures including but not limited to the Data Privacy guidelines, Information Security Policy, Code of Conduct and Disciplinary Action Policy during WFH.
- Be contactable during the normal span of hours.
- Not everyone has a designated home office, but it is critical to have a private, quiet space for your work. If you can, separate your work area from your personal spaces and use it just for work, not for other activities.
- Make sure to set boundaries with family members.
- Ensure family members understand that although you are home, you are working.
- Establish ground rules for work hours, interruptions, noise, etc.
- Try that any household items/family members are not visible during a video conferencing.
- Adhere to clear desk and clear screen policy.
- Employees should refrain from using any Social Networking website, streaming websites, and any websites, which contains video contents.
- Lock system when stepping away from workspace.
- Employees must not capture snap, copy/paste, print, save on local storage (Hard Drive, USB, DVD etc.)

Dos and Don'ts for employees while working outside Office Premises

Dos	Don'ts
Report Security incident if you think there is a breach.	Don't ignore security policy. Ignorance doesn't mean it doesn't apply to you.
Know and meet your legal obligation towards clients and suppliers.	Don't open unsolicited e-mail attachments without verifying their source.
Ensure that your machine has latest patches and anti-virus updates. Take IT ops help.	Don't write password on post-it sticker or desk or under key board.
Beware of 'shoulder-surfers' while you login. Be vigilant and look out for phishing emails, which could leak confidential information	Don't discuss customer information in public areas.
Back up your files on a regular basis.	Don't expose data-media to environmental hazards.
Log out of applications/web services before closing the page/browser.	Don't divulge personal information without verifying source.
Lock your screen (CTL+ALT+DEL+ENTER) before you leave your workstation.	Don't throw documents/media in dustbins. Destroy them properly to avoid dumpster-divers.

Working with PI (Personal Information) and SPI (Sensitive Personal Information)

The Company respects the privacy of all its employees, business partners and customers. We must handle PI and SPI responsibly and in compliance with all applicable privacy laws. Users who handle the personal data of other employees, clients and vendors must:

- Act in accordance with Coforge Data Privacy Framework available on iEngage.
- Act in accordance with any relevant contractual obligations.
- Collect, use, and process such information only for legitimate business purposes.
- Limit access to the information to those who have a legitimate business purpose for seeing the information.
- Take care to prevent unauthorized disclosure.

Code of Practice for Use

In Office

- Users should lock their computers when they leave their desk.
- Users should avoid discussing PI/SPI in person or over the telephone when they are within earshot of anyone who does not need to know the information.
- Users must never leave PI/SPI unattended on a desk, network printer, fax machine, or copier.
- Users should not leave the PI/SPI in a location where another individual (e.g., writing one's PI on a note affixed to one's monitor or keyboard) can readily obtain it.
- Users should use a privacy screen if they regularly access PI/SPI in an unsecured area where those without a need to know or members of the public can see user's screen, such as in a reception area.
- Users are not permitted to post SPI on company intranet, SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know."
- Users should physically secure PI/SPI when not in use or not otherwise under the control of a person with a need to know.
- Users should store SPI in a space where access control measures are employed to prevent unauthorized access by members of the public or other persons without a need to know (e.g., a locked room or floor, or other space where access is controlled by a guard, biometrics, or card reader).
- Users are not permitted to access and use the PI/SPI for reasons unrelated to their job.
- Users should protect the unprotected PI/SPI shared by someone in the same manner, as the PI/SPI handled by them.
- Users should ensure that PI/SPI are shredded/disposed securely.

When working from Home

- Users must access PI/SPI only via Coforge approved Portable Electronic Devices (PED) such as laptops, phones, USB flash drives, and external hard drives,
- Users should not use personal PEDs to access, save, store, or host PI/SPI unless they log in through the Coforge provided VPN.
- Users are not permitted to transfer files to their home computer or print company records on their home printer.
- Users should not forward emails containing PI/SPI to their personal email account (e.g., their Yahoo, Gmail, or AOL e-mail account) so that they can work on it on their home computer.
- Users must obtain authorization from their supervisor to remove documents containing PI/SPI from the office.
- Users must secure their PED and any hard copy PI/SPI while working from home and ensure that other household members cannot access them.

When Travelling

- Users must access PI/SPI only via Coforge approved Portable Electronic Devices (PED) such as laptops, phones, USB flash drives, and external hard drives,
- Users should not use personal PEDs to access, save, store, or host PI/SPI unless they log in through the Coforge provided VPN.
- When transporting laptop or Portable Electronic Device (PED):
    - If user must leave the PED in a car, user should ensure to lock it in the trunk so that it is out of sight. Users should never leave their laptop or PED in a car overnight.
    - Users must not store a laptop or PED in an airport, a train or bus station, or any public locker.
    - Users should avoid leaving a PED in a hotel room. If they must leave it in a hotel room, they should lock it inside an in-room safe or a piece of luggage.
    - At airport security, users should place their laptop or PED on the conveyor belt only after the belongings of the person ahead have cleared the scanner. If delayed, users must keep an eye on it until they can pick it up. Users should not place a PED in checked luggage.
    - If the PED is lost or stolen, users must report it as per company's Incident/Security Incident management processes.

Removable Media Usage

- The use of removable media for storage of Coforge / Client information must be supported by a reasonable business case including approval from Delivery Head & Information Security Team.
- All removable media use must be approved by Delivery Head & Information Security Team before use.
- Personally, owned removable media use is not permitted for storage of Coforge / Client information.
- Company or Client provided information should not be stored on removable media device until the same has been approved. If to be stored, then the same must not be without the use of encryption.
- The loss or theft of removable media device that may have contained any Coforge / Client information must be reported to the Information Security Team.

Social Media Usage

- Communications made with respect to social media should be made in compliance with all applicable Coforge policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Coforge, including accounts that could reasonably be assumed to be an official Coforge account, requires the permission of the Coforge Marketing Team.
- Personnel should not misrepresent their role at Coforge.
- Personal information belonging to customers should not be published online.
- When discussing Coforge or Coforge -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Coforge representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Coforge unless you have been explicitly approved to do so.
- When publishing Coforge -relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be "The opinions and content are my own and do not necessarily represent Coforge's position or opinion."
- Content posted online should not violate any applicable laws (i.e., copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, colour, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with Coforge will not be tolerated.
- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.
- Personnel approved to post, review, or approve content on Coforge social media sites must follow the Coforge Policies and Procedures.

Security Training and Awareness

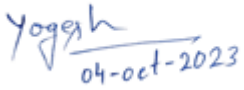
- All new joiners must complete the approved security awareness training prior to, being granted access to any Coforge Information Resources.
- All personnel acknowledge & agree to adhere to the Coforge Information Security Policies.
- All personnel must complete the mandatory security awareness training annually.

Yogesh
04-oct-2023

IR 123 Acceptable Use Policy

Coforge

Disclaimer: "I hereby declare that I have gone through all the terms and conditions mentioned in the Acceptable Use Policy (AUP) and I accept the same.



Place: Greater Noida

Date: 04/10/2023 **SIGNATURE / THUMB IMPRESSION OF EMPLOYEE**

Employee Name: _Yogesh_____

Revision History

Sr. No.	Ver No.	Prepared By	Reviewed By	Revision Date	Approved By	Approval Date	Reason for new release
1	1.0	KK Chaudhary	IST	-	Resource Head - SSB	23 Mar 2009	Initial Issue
2	1.1	Tapan Chowdhury	KK Chaudhary	18 Mar 2010	Resource Head - SSB	30 Mar 2010	Revision History Table added
3	1.2	Tapan Chowdhury	KK Chaudhary	23 Jun 2010	Resource Head - SSB	23 Jun 2010	Updated "Code of Practice" for Email and Internet uses
4	1.3	Tapan Chowdhury	Arun Kumar Anand	25-Jul-2012	Resource Head - SSB	14-Sep-2012	Reviewed and changes made in the document as required
5	1.4	Tapan Chowdhury	Arun Kumar Anand	18-Sep-2013	Resource Head - SSB	19-Sep-2013	Policy included to restrict use of "Crack" files and "License key generator".
6	1.5	IST	Arun Kumar Anand	22-Sep-2014	Resource Head - SSB	22-Oct-2014	Policy amended to include "Laptop Encryption".
7	1.5	IST	Arun Kumar Anand	30-Sep-2015	Resource Head - SSB	30-Sep-2015	Reviewed and no changes.
8	1.6	IST	Arun Kumar Anand	17-Mar-2016	Resource Head - SSB	23-Mar-2016	Policy amended to include DLP and CF and prohibited websites.
9	1.7	IST	Arun Kumar Anand	24-Feb-2017	Arvind Mehrotra	27-Feb-2017	Policy updated to include Acceptable Use of Office 365
10	1.7	IST	Arun Kumar Anand	28-Jan-2018	President IMS	05-Feb-2018	Policy amended to update Approval Authority names for DLP deployment.
11	1.8	IST	Arun Kumar Anand	18-April-2018	Arvind Mehrotra	24-05-2018	Policy updated to include GDPR clause.
12	1.9	IST	Tarun Malik	22-Feb-2019	Vamsi Krishna	19-Mar-2019	1. DLA replaced with IT Support 2. President IMS replaced with IMS Head

13	2.0	IST	Jitendra Mohan Bhardwaj	03-Mar-2020	Ajay Kalra	18-March-2020	• Policy amended to include mobile encryption & Intune algorithm. • In GDPR Act updated as per the Coforge data privacy framework. • Legal hold functionality included for O365 application only in India Stakeholder.
14	3.0	IST	Jitendra Mohan Bhardwaj	04-Sept-20	Ajay Kalra	14-Sept-20	Changes in line with company is rebranding to Coforge Limited.
15	3.1	IST	Jitendra Mohan Bhardwaj	20-May-21	Ajay Kalra	10-June-21	• Work from home guideline added. • Dos and don'ts for employees while working from home during Pandemic
16	3.1	IST	IST-Lead	02-May-22	Jitendra Mohan Bhardwaj (CISO)	13-May-22	Reviewed but no changes made
17	3.2	IST	IST – Lead	04-Jan-23	Jitendra Mohan Bhardwaj (CISO)	04-Jan-23	Disclaimer added
18	3.3	IST	IST – Lead	1st May 2023	CISO	12th May 2023	Inclusion of • Purpose • Scope • Acceptable Use • Social Media Usage • Removable Media Usage • Security Training and Awareness.

About Coforge

Coforge is a global digital services and solutions provider, that enables its clients to transform at the intersect of domain expertise and emerging technologies to achieve real-world business impact. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct perspective. Coforge leads with its product engineering approach and leverages Cloud, Data, Integration and Automation technologies to transform client businesses into intelligent, high growth enterprises. Coforge's proprietary platforms power critical business processes across its core verticals. The firm has a presence in 21 countries with 25 delivery centers across nine countries.

Learn more: www.coforge.com

For more information, contact information@coforge.com

Coforge