ACCEPTABLE IT USAGE POLICY

Capgemini India

India

Cybersecurity

Version:	4.9
Status:	Published
Usage:	All rights reserved
Author:	Anand Sumant & Srinivas Sharma
Date:	08/09/2021

Approval			
Organization	Name (Function)	Date	Document Version
Group IT APAC	Mr. Amisagadda Seshaiah- AD – ITICS	08-08-2004	1.0
Group IT APAC	Mr. Amisagadda Seshaiah -AD – ITICS	20-01-2005	1.1
Group IT APAC	Mr. Amisagadda Seshaiah	29-01-2005	1.2
Group IT APAC	Mr. Amisagadda Seshaiah-AD – ITICS	12-03-2005	2.0
Group IT APAC	Mr. Amisagadda Seshaiah-AD – ITICS	01-12-2005	2.1
Group IT APAC	Mr. Amisagadda Seshaiah-AD – ITICS	16-10-2006	3.0
Group IT APAC	Sudarshan Singh- AD-ISMS	19-09-2009	3.1
Group IT APAC	Mithilesh Singh- Information Security Officer	23-09-2010	3.2
Group IT APAC	Sudarshan Singh- Director – ISMS	15-07-2011	3.3
Group IT APAC	Sudarshan Singh- CISO	28-07-2012	3.4
Group IT APAC	Sudarshan Singh- CISO	05-08-2013	4.0
Group IT APAC	Sudarshan Singh- CISO	8-07-2014	4.1
Group IT APAC	Sudarshan Singh - CISO	02-08-2015	4.2
Group IT APAC	Sudarshan Singh - CISO	16-08-2016	4.3
Group IT APAC	Kalpesh Doshi - CISO	04-05-2017	4.4
Group IT APAC	Kalpesh Doshi - CISO	13-07-2018	4.5
Group IT APAC	Sarvesh Dhuri – GRC APAC Lead	22-10-2018	4.6
Group IT APAC	Sudarshan Singh - CISO	16-07-2019	4.7
India Cybersecurity	Deepak Kulkarni	24-08-2020	4.8
India Cybersecurity	Deepak Kulkarni	3-09-2021	4.9

Distribution		
Organization	Recipients	Document Version
Group IT	Capgemini India – ISMS	1.0
Group IT	Capgemini India – ISMS	1.1
Group IT	Capgemini India – ISMS	1.2
Group IT	Capgemini India – ISMS	2.0

Group IT	Capgemini India – ISMS	2.1
Group IT	Capgemini India – ISMS	3.0
Group IT	Capgemini India – ISMS	3.1
Group IT	Capgemini India – ISMS	3.2
Group IT	Capgemini India – ISMS	3.3
Group IT	Capgemini India – ISMS	3.4
Group IT	Capgemini India – ISMS	4.0
Group IT	Capgemini India – ISMS	4.1
Group IT	Capgemini India – ISMS	4.2
Group IT	Capgemini India – ISMS	4.3
Group IT	Capgemini India – ISMS	4.4
Group IT	Capgemini India – ISMS	4.5
Group IT	Capgemini India – ISMS	4.6
Group IT	Capgemini India – ISMS	4.7
India Cybersecurity	Capgemini India	4.8
India Cybersecurity	Capgemini India	4.9

Updates

Version	Date	Author	Description of changes
1.0	08-06-2004	C. Rai – ISMS Manager	FIRST RELEASE
1.1	15-01-2005	C. Rai – ISMS Manager	Second Release – Revision of earlier release to adapt QMS guidelines on document controls and classification standard
1.2	28-01-2005	C. Rai – ISMS Manager	Control 3.9 – “network” was replaced with “network server”
2.0	3-03-2005	CRAI – ISMS Manager	SECOND RELEASE
2.1	27-09-2005	Chandrashekhar Moharir – ISMS Team	Changes in software copyright compliance, Internet policy, maintaining information security, password policy.
3.0	04-10-2006	Cmoharir- ISMS team	THIRD RELEASE
3.1	19-09-2009	Kamal Seepana- ISMS Team	No changes
3.2	02-04-2010	Daksha Malli	Policy Revision

3.3	28-06-2011	Rudraksha Chodankar	Edited the controls 2.4, 2.5, 2.6, 2.7, 2.10 and 2.11 under maintaining information security, 4.1 and 4.2 under clear desk and clear screen policy. Removed the controls 5.2 and 5.7 under system password usage policy. Minor changes to section 3, 6, 7 and 8. Section 9.5 changed
3.4	15-07-2012	Manish Kamble	Addition of Customer Security Requirements in Control 1 Document Purpose and Compliance, Addition of Online Mass storage category in Control 2 (2.15), Edited Control 3 Copyright Compliance, Addition of Control 7 Email- Active Sync Configuration Policy for Mobiles and Control 12 Access to XS4MOBILES and XS4GUEST
4.0	17-07-2013	Sarvesh Dhuri	Minor changes in point no. 2.7 , 2.8 , 2,12 , 5.3 & Section 15
4.1	7-07-2014	Sarvesh Dhuri	Added references of customer provided services such as Internet and Email Service in relevant sections. Changed the ITICS Helpdesk Number.
4.2	02-08-2015	Ashwini Abhyankar	Changed ISO 27001 mapping from 2005 to 2013 edition. Template changes as per new template document template. Replaced 'third party' terminology to supplier. Added Google Hangouts in 4.6.6 section. Scope of the policy aligned based on ITICS East support coverage. Further clarity on Clear Desk policy.
4.3	16-08-2016	Sarvesh D	No Changes
4.4	29-04-2017	Sarvesh D	Section 2 – Scope updated to reflect Group IT APAC Section 4.5 – Addition of Mobile device management
4.5	30-06-2018	Rajesh Hariharan	Template upgrade.
4.6	22-10-2018	Rajesh Hariharan	Added statement on mandatory Information Security training under section 4 "Minimum standards for Acceptable IT Usage policy"
4.7	11-07-2019	Srinivas Sharma	Updated the Data Classification details under section 4.3 Clear Desk & Clear Screen. Other minor changes
4.8	9th August 2020	Ashwini Abhyankar	Updated the ownership of the document to the India Cybersecurity team. Minor changes in section 4.1, 4.10, 4.11 & 4.10. Included user responsibilities about Operating System updates, Security patches and Antivirus definitions under section 4.1.
4.9	8th September 2021	Anand Sumant & Srinivas Sharma	Reviewed the document. Updated the template. Changes to section 4.2 Minor change in the purpose, scope, section 4.11, 5

Storage		
URL	Anonymous access?	Manager
India Cybersecurity SharePoint portal	No	Nilesh Panditrao, Srinivas Sharma & Anand Sumant

Reference Documents			
S No	Document Name	Location	Owner
1	ISO 27001:2013 – Control Objective: A.6.2, A.7.2, A.8, A.9.2, A.12.5.1, A.12.3, A.11.2, A.12.6, A.13.2.3, A.18	ISMS Standard	India Cybersecurity

1 Table of Contents

1. Purpose

This policy is issued with authority of the Information Security Forum (ISF) also known as Steering Committee and owned by **Capgemini Technology Services India Ltd. (Capgemini India)** Cybersecurity Officer CSO. Compliance is mandatory for all users (employees, sub-contractors, suppliers) having access to any of facilities or information systems or information owned or processed by Capgemini. This "Acceptable IT Usage Policy" is an extension of the "ISMS Policy Manual". The purpose of the policy is to protect the information assets owned and processed by the Capgemini India from all threats, whether internal or external, deliberate or accidental, to meet all business, regulatory and legislative requirements. This document forms part of the organization's initiative to achieve and continued compliance to ISO 27001:20013.

2. Scope

This policy shall be applicable to employees, sub-contractors and suppliers, vendors hereafter referred as "the user". This policy is applicable for Capgemini India managed geographies. This policy shall also be applicable for users delivering services from customer location using Capgemini assets/ information resources. This policy is applicable to all users while even working on customer network connected by means of direct connectivity or through VPN using Capgemini Network. In case the customer security requirement supersedes Capgemini Acceptable IT Usage policy, the user shall follow customer security requirements. In case, security requirements of the customer are not meeting the requirements of Capgemini Acceptable IT Usage Policy, in such cases the users are required to follow this Acceptable IT Usage Policy. Any exception to the requirement needs to be referred to ISMS with business justification and relevant approvals. Such exception will be considered after risk assessment of such exception to overall IT environment and security control framework.

This policy document shall be published on the Organization's Intranet or central repository accessible to all the employee. In the event of an issue arising from an interpretation of this policy document, it will be resolved by ISMS function.

3. Non-compliance

Where a breach of the "Acceptable IT Usage Policy" is established, one or more of the following penalties may be imposed on a user responsible for, or involved in the breach:

- Warning
- Formal written warning
- Restriction, revocation or termination of access to Capgemini network
- Disciplinary actions, which may include dismissal of the employee or termination of a contract

Any action taken internally does not preclude prosecution under relevant laws

4. Minimum standards for Acceptable IT Usage Policy

4.1. Information Assets

Maintaining Information Security is each user's responsibility. The user must understand security requirement within their functional domain and strive to protect information assets with highest priority. In any case of conflict understanding or loss of understanding, the same should be referred to ISMS function for clarification

1. Employee shall not disclose information relating to the Organization's IT facilities to anyone outside the organization without the organization's permission. Any information searching efforts by outsider shall be communicated to immediate manager or ISMS function
2. The user will be provided company assets (desktop, laptop, authentication tokens, phones etc.) and information systems or services access (internet, PSTN, VoIP, customer's system, VPN, VDI profiles intranet etc.). The assets and services should be used for delivering services to the company and should be used appropriately. The user should ensure security of such access. Any misuse of these assets or access will be attributed to the user only.

3. While Group IT would distribute the Operating System updates, security patches and Antivirus definitions to all computers, the users will have an obligation to report to Group IT in case the updates are not happening.
4. The user will be provided access to its customer's IT systems and services (email, internet, business information systems etc.). These accesses must be used for delivery services to the customer; its usage must also be governed by the customer's information security policy. Any all cases, most restrictive policy shall prevail. In case of any ambiguity on such use, the user should seek clarification from its project manager or the customer. Any misuse of such services shall be treated as violation of customer and Capgemini Acceptable IT Usage Policy
5. The user shall make oneself aware of information classification procedure as defined in ISMS Policy Manual. The user must follow and ensure controls as mandated in dealing with "Company Confidential", "Company Restricted" and "Company Sensitive" information
6. The user must not send any information classified or having classification attributes of information as "company confidential", "customer confidential" and "sensitive" to its personal email. Such email transactions are subject to monitoring by Data Leakage prevention tool & in case of any violation, it shall be treated as security incident.
7. Sensitive, Company Confidential and Customer confidential information must not be copied on to any personal device or stored to any non-approved cloud-based file storing & sharing platform /websites.
8. Computers logged on to the network shall never be left unattended. Users shall ensure that their computers are secured from un-authorized access. The user shall be held accountable for any misuse of their computer or computing resource.
9. The user must not attempt to access a system to which one have no authorization.
10. Project related data must be saved on a company's information repository (network drive on file server, share point portal, T-Rooms). The only circumstances where project related data may be saved to the hard disk, is when a laptop is being taken to a site where the organization's network is inaccessible, and data is required for business purposes. However, in such case, the end user will be accountable responsible for safekeeping and security of the data stored on laptop.
11. Only Group IT is authorized to move any IT equipment, within an office or to another site. User should not themselves move any IT equipment. The following may not be installed or configured on any computer other than by Group IT (a) peripheral devices of any kind (digital cameras, PDA's, modems, etc.) and (b) removable media devices including CD writers, tape backup, memory sticks, flash cards, USB memory, Bluetooth storage and other devices. The mentioned list is not exhaustive and includes all other removable memory and media devices. (c) Wireless router or any WIFI infrastructure
12. Disposal of IT equipment shall be arranged by GROUP IT with due consideration of legal (software compliance) and environmental issues. No user shall dispose any IT equipment.
13. User shall not disable, circumvent or disrupt working of any security controls (Anti-malware, GPO, Patch, Encryption, web filtering etc.) which are by default a part of standard configuration
14. Capgemini India has deployed encryption solution on all its laptops, in order to safeguard information stored on laptops. It is the user's responsibility to inform GROUP IT / ISMS if its laptop is not encrypted or encryption solution is not working.
15. Online mass storage facility (Public version of Drop box/Sync/ Rapid Share/ Google Docs/ GitHub/Bitbucket etc.) shall not be permitted for storing "company confidential", "sensitive" and "customer confidential" information. Specific projects that require access to such websites shall take approval from the customer and ISMS before using it.
16. All Capgemini employees are required to undertake Cyber Security, Information Security and Data Privacy trainings as defined in polices. These are provisioned in the form of CBT / online training courses. Easy reference to same is below:

5 Modules

- U-EE-CYSIP-CEIESM – Internet, Email, and Social Media
- U-EE-CYSIP-MRT - Cybersecurity 2/5: Cyber Risks and Threats
- U-EE-CYSIP-WSEN - Cybersecurity 3/5: Working Securely Everywhere
- U-EE-CYSIP-DPCN - Cybersecurity 4/5: Data Classification and Security
- U-EE-CYSIP-RSI - Cybersecurity 5/5: Reporting Security Incidents

4.2. Copyright Compliance

1. Copyright law, which governs the use of intellectual property, including software, is very straightforward – it is illegal to copy or reverse-engineer any software unless expressly permitted by the copyright holder. The organization may face legal prosecution as consequences of illegal usage of software. Legitimate copies of software will be promptly provided to all users on need basis by Group IT, subject to the necessary authorization.
2. The user shall not make any copies of software under any circumstances without explicit written permission of the Group IT.
3. Any user illegally reproducing software or using software that is found to have been illegally reproduced may be subject to legal action including all applicable legal penalties, in addition to the organization's disciplinary procedure
4. No User shall give any organization software to any outsiders, including customers unless authorized by GROUP IT
5. Any User, who determines or suspects misuse of software within the organization, shall notify Group IT Helpdesk and ISMS function.
6. All software must be purchased through IT Procurement function.
7. Users are strictly prohibited from installing any software by downloading it from internet or by any unauthorized means like copying from external media like USB drives or hard disk. Any software other than company/ customer provided found in systems shall be treated as violation of policy.
8. Installation of third-party applications, games, peer-to-peer file sharing software, freeware, download of bandwidth intensive audio/video files, chat software other than for business and official use is strictly prohibited.
9. All software, information, programs and code developed for and/or on behalf of Capgemini or with the use of computers and other applications which are the property of Capgemini by employees/contractor shall remain property of or considered property of the organization or the customer for whom the software was developed. Duplication or sale of such software without the prior consent of Capgemini India shall be an infringement of the Capgemini India's copyright and will be dealt with as a disciplinary matter.
10. End Users are advised to read and adhere to **Capgemini Group IT's Software Usage Policy** to understand Software Classification and End user responsibilities on using Software.
11. For using Open Source Software, it is recommended that end users refer to the Capgemini Legal **Open Source Policy** and take consent from their Engagement/BU Legal prior to using, such that their usage does not violate i) Open Source Software terms of use ii)Customer contracts both Existing and New.

Exception Handling: If for any reasons Business needs to use one or many software products in their Project deliverables without a valid source, for e.g., Customer Loaned, Alliance Provided, Business purchased etc., then in such cases the engagement should perform a Risk Assessment with the help of BU CISO and Engagement Legal to identify current possible and future probable risks arising out of such usage and document a Risk Management Plan. Such Risk Management plan should demonstrate the engagement's acceptance of Risks and responsibility towards all related impacts, including but not limited to costs & penalties for software licensing, legal matters, statutory compliances etc.

No user shall install any virtual instance on any of the workstation or server without proper approval and authorization from GROUP IT.

4.3. Clear Desk & Clear Screen

1. Each User shall maintain CLEAR DESK policy. No printed documents or soft media (CD/DVD/USB Storage) classified as "Company Confidential ", "Company Restricted", "Customer Restricted", or "Company Sensitive" shall be kept in public view or open desk. Printed copies of all such classified documents must be shredded before disposal; classified documents including customer-supplied documents shall be kept under lock and key.
2. Users shall ensure that they lock their computer screen with password before leaving the work desk to avoid unauthorized viewing or access of computer data.

3. Sticky notes or confidential data having any information like IP address, ID/ passwords or source code shall not be stored on desktop to avoid data leak through shoulder surfing or any social engineering attack.

4.4. Password

1. The user shall be provided with unique named credential (username and password); it must not be shared with any other user, third party or outsider. Passwords shall not be written down. The user shall ensure that system access passwords given to them by customer shall be used in conformity with customer password usage policy and guidelines. At minimum, these passwords shall not be shared with other users within or outside the team until and unless explicit permission is obtained from customer and immediate manager. Such permission should be kept in record and available for audit purpose.
2. The user must take appropriate precautions to prevent others from obtaining access to their mobile device(s) configured for company access. The user will be accountable for all transactions made with their credentials, and should not share individually assigned passwords, PINs or other credentials.
3. All project related servers including database whether in test function or production environment, shall be configured with unique user id and password.
4. Here is an illustrative list of "do's and don'ts" in dealing with password and authentication credentials.
    - Do not use the same password for internal system (domain account -Capgemini) and external system access (e.g. customer provided systems, personal accounts).
    - Do not share your user id and passwords with anyone, including team members. All passwords are to be treated as "sensitive" information.
    - Do not reveal a password to anyone in any means not limited to phone, email, fax, etc.
    - Do not hint at the format of a password (e.g., "my family name").
    - Do not reveal a password on questionnaires or security forms.
    - If someone demands a password, refer him or her to this document or have him or her connect to ISMS.
    - Do not use the "Remember Password" feature of applications (e.g., Outlook, public email systems, Internet explorer etc.).
    - Do not enable "Auto Form Fill" feature of the web browser. These features are vulnerable as they cache the sensitive information on the local machine. If compromised, this information can be easily accessed by the unauthorized person.
    - Avoid using other person's workstations to access sensitive applications, Capgemini network, customer database, internet banking, e-commerce, etc. as far as possible. There may be KEYLOGGER or other SPYWARE programs running in stealth mode to capture account detail and password.
4. If an account or password is suspected to have been compromised, report the incident to ISMS function (securityincident.in@capgemini.com.or Group IT helpdesk on 4004) and immediately change all passwords

4.5. E-Mail

1. The company provides e-mail services to assist employees in the performance of their jobs. Its use shall be limited to company business. While working on customer network, customer provided email services shall strictly be used for official purposes only. Capgemini India reserves the right to purge identifiable personal e-mail to preserve the integrity of its e-mail systems. User shall not use the Organization's e-mail system in any way that may be interpreted as insulting, disruptive or offensive by any other person, or company, or which may be harmful to organization ethics. This includes forwarding any received e-mail, sending mass mailing emails for personal reasons, etc.

   Examples of prohibited material and prohibited use of organization email include:

    - Sexually explicit messages, images, cartoons, or jokes.
    - Unwelcome propositions, requests for dates, or love letters.
    - Profanity, obscenity, slander, or libel.
    - Ethnic, religious, or racial slurs.
    - Political beliefs or commentary.
    - Threat or abuse mail

- Other communications which may directly or indirectly result in.
  - Copyright infringement
  - Disclosure of confidential information
  - Transmission of computer viruses
  - A breach of any law
  - Any information which may compromise information security of the company or any message that may be constructed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

2. All emails sent outside Capgemini domains are subjected to monitoring. In case of breach of policy, incident shall be triggered and escalated to the line manager and appropriate management level & Human Resource for further investigation and necessary actions.
3. All e-mail sent or received are logged and may be stored for future reference. These emails may be opened and read by a duly authorized officer of the company.
4. Forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. In addition, virus warning comes under the same inclusion. If you wish to check the authenticity of these messages, it should be referred to India Cybersecurity ISMS (spambox@capgemini.com). But under no circumstances; it should be forwarded to anyone inside or outside the organization.
5. No messages of any kind shall be sent to multiple external destinations. This may be considered as 'spamming'. In all messages, it should be remembered that e-mail is not a secured form of communication. The sent messages will pass over networks owned by other entities. If the content of the message can create problems for the Capgemini India on content being known, a more secure method should be used by the user. The same can be consulted with ISMS. Users shall ensure that all outgoing e-mail contains standard company disclaimer.
6. The user logged in at a computer shall be considered author of any messages sent from that computer. User must log-out from or lock their computer, if away from its desk.
7. E-Mail addresses shall not be unnecessarily disclosed. If the user provides one's work email when filling in surveys or in other questionnaires, user will be at risk of receiving unwanted junk and spam messages. It may lead to disruption of services or unwarranted use of company resources.
8. The user shall not subscribe to e-mail lists, which are not in organization's interest and such subscription should not be in violation of "terms & conditions" by the service provider.
9. The user shall not subscribe to professional networking sites using company email id
10. The user shall not subscribe to email list, where content is inappropriate and objectionable. The broad category of objectionable content is illustrated in clause 4.5. point 1
11. Be aware of phishing mail/s. Phishing message will often ask you to take an action such as clicking a link, opening an attachment, or responding with sensitive data. The user shall not open attachments to e-mail messages unless one is expecting them or the emails are coming from known source, and even then, should exercise extreme caution when doing so. The user shall always scrutinize the website address or sender's email address carefully to find anomaly. Any Capgemini web site must be accessed using browser and not through clicking on any weblink coming from external email. Any suspected Phishing emails Create a new email by clicking forward as an attachment to spambox@capgemini.com with subject as **'Phishing Attempt'**.
12. The facility to automatically forward e-mails shall not be used to forward messages to personal e-mail accounts. Capgemini India provides many solutions for accessing the Capgemini India's e-mail system when away from the office.

4.6. Internet Usage Policy

1. Capgemini India provides Internet services to all users to assist them in performance of their jobs. Internet Usages policy shall be applicable to the users even the user is availing internet services through customer network or customer hosted internet gateways.
2. No messages shall be posted on any internet message board or other similar web-based service or any social networking sites that would bring the company or customer into disrepute, or which a reasonable person would consider offensive or abusive. The list of prohibited materials is the same as illustrated in section 4.5. point 1. Even though user may not leave one's name, other identification method exists, including the address of the computer they are using, which may still allow others to locate the organization that the user belongs to, and the particular computer used to post a message. The user shall not engage in any illegal activities using the internet. The system shall not be used for personal gains, nor shall user host a personal web site on any company's equipment

3. The user shall not participate in on-line games or have active any web channel that broadcasts frequent updates on user's computer, such as the news broadcasts, match scores, exchange prices etc.
4. The user shall not visit web sites that display material of a pornographic nature, or which contain material that may be considered offensive or objectionable. The objectionable content is illustrated in the section 4.5. point 1
5. The user logged in at a computer will be considered the user using the internet. It is the responsibility of user to logout from or locks one's computers.

4.7. Data backup and restore policy

1. The user is required to save all business-related data on centralized storage facilities provided by Group IT (for example central file server, Team Forge or T-room, SharePoint etc.) GROUP IT is not responsible to take backup of data on user workstations and laptops.

4.8. Mobile & Tele-working Policy

4.8.1. The users shall ensure safety of the company assets (laptop, smartphone, authentication token) allocated to them at all times.
4.8.2. Connecting to Organization's network from remote location shall only be allowed through pre-defined authentication and authorization mechanism
4.8.3. User should not attempt to dial-in or connect to Internet using data card when they are connected to Capgemini network.
4.8.4. Users shall ensure that while accepting visitor within the company premise, they should help the visitor declare any electronic media such as laptop, CD, hard drive, USB or flash drive. Laptops shall not be left on the desk or in the work area overnight. Users shall not leave laptop unattended in cars or in public area like airport and hotel lounge. Laptop shall not be checked-in as baggage

4.9. Mobility Policy

1. Depending upon work responsibilities, the user may be provided internet connection and accessibility of office mail through data card modem or /and GPRS (General Packet Radio Service) or/and Smartphone using Mobile device management solution. The controlled use of the service or facility shall be sole responsibility of the user and any liability arising due to inappropriate use will be of the user only.
2. Only standard provision-able devices are allowed. Please refer to Group Cybersecurity Personal Device Policy.
3. The company provided Internet connectivity medium shall be used only for legitimate business purpose.
4. The mobile internet connectivity may enable an uncontrolled access to internet. Even in such case, Internet policy as mentioned in section 4.6 should be applicable.
5. The users are responsible for safety and secured use of the IT assets, services and resources. In case of any missing or stolen device, user is required to notify regional GROUP IT Asset, ISMS and Group IT helpdesk
6. When connecting the Personal Device (smartphone and tablets) to Capgemini systems, the Capgemini' applicable security Policies shall be enforced on the Personal Device at all times. The Security Policies implemented may include, but are not limited to, areas such as passcode, passcode timeout, passcode complexity and encryption.
7. In case your Personal Device is lost, stolen or has been hacked, you must contact, within 24 hours, GROUP IT Service desk so that the appropriate security measure, including erasure of the Capgemini Information can be taken. The employee personal device may be remotely wiped by Capgemini if 1) the personal device is lost, 2) employment is terminated for any reason, 3) Group IT detects a data or Policy breach, a virus or similar threat to the security of the Capgemini Information and technology infrastructure.
8. Capgemini India retains the right to remotely erase any Capgemini Information stored in the personal device for any reason and without any prior notice for technical reasons or for the protection of Capgemini Information. Capgemini cannot be held liable for erasing Employee Information when it is required for technical reasons or for the protection of Capgemini Information.

4.10. Access to Corporate WIFI infrastructure

1. Non-company devices (such as smartphones/tablets) may be connected to mobile profiles. Employees needing access to mobile profile shall require providing specific business justification and their line manager approval. Such access shall be enabled by additional authentication mechanism.
2. Customer laptops, tablet and smartphones shall be connected to Guest Wi-Fi network for a limited duration not exceeding 5 days. Access to guest wireless network shall be provided only to customer and external third party (for example auditors) with business justification. The user credential (user ID and password) will be unique to the user.
3. Users are not allowed to setup wireless infrastructure or create ad-hoc network

4.11. Social Networking and Social Media Sites Policy

Social networking sites are online virtual community on the internet sharing common interest or common attributes (like Organisation, friends, technology domains etc.). Some of the popular social networking sites are Facebook, Twitter, Yammer, LinkedIn, Flickr, YouTube, etc. These sites are gaining popularity and been used as efficient tools for knowledge sharing or opinion sharing on a subject or interest. However, improper use of these will lead to information security breach resulting into security incidents which can cause reputational damage or information loss. Some of the websites are blocked on Capgemini India Internet Gateways & access is granted to users only with appropriate business justification and approval from relevant authorities.

The user needs to adhere to the below guidelines:

1. Social networking must be done in a professional and responsible manner.
2. Public statements about Capgemini must be approved by Corporate Communication.
3. The Capgemini Group's or its customer's confidential or proprietary information, trade secrets or any other material covered by the Capgemini Group's or its customer's confidentiality policies must not be revealed. The user must refrain from quoting its engagement with specific customer to customer's project
4. Employees should not identify themselves as a representative of Capgemini.
5. Publications and social networking should not be detrimental to the Capgemini Group's, its customer's and third parties' interests, and shall not interfere with any employee's regular work duties.
6. Any personal posts and/or referral, recommendations for a friend or employee made by such employees on these sites shall be considered as personal opinions expressed solely by the author and do not represent the view of the company.
7. The user shall comply with copyright and fair use of the media,
8. The user shall show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory for example sexual orientation and religion, ethical, obscenity. Company logos and trademarks shall not be used without written consent.
9. Uploading of company/client owned information/data on social networking public platforms/repositories is strictly probhited.

5. Reporting of security incident:

All users (employees, contractors, sub-contractors) are responsible to report all security incidents to ISMS. Few examples of information security incidents are:

- Unauthorized access or disclosure
- Misuse of Information Assets
- Falsification of Information
- Theft, damage, or destruction of information assets
- Breach of security policy
- Sharing of source code, client or Capgemini data to any unauthorized sharing platform such as GitHub, Bitbucket, Box drive, or other cloud or non-cloud storage platforms

You are required to immediately report any incidents to the Group IT Help Desk 022-67557744, if you are in office dial on 4004 or email to "IN, securityincident" securityincident.in@capgemini.com or IN, ISMS ISMS.in@capgemini.com

Intentionally left blank

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 270,000 team members in nearly 50 countries. With its strong 50 year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion.

Get the Future You Want | www.capgemini.com