Acceptable IT Usage Policy

Capgemini India

The information contained within this document is the property of CAPGEMINI INDIA and is issued in confidence and must not be reproduced in whole or in part.

Document Control

Revision History

Date	Version	Author	Description
8th June 2004	1.0	C. Rai – ISMS Manager	FIRST RELEASE
15th Jan 05	1.1	C. Rai – ISMS Manager	Second Release – Revision of earlier release to adapt QMS guidelines on document controls and classification standard
28th Jan 05	1.2	C. Rai – ISMS Manager	Control 3.9 – "network" was replaced with "network server"
12th Feb 05	1.3	CRAI – ISMS Manager	Addition of control 3.19 "Network access to temporary employees and visitors" under section 3 Addition of SECTION 8 "Mobile computing and Teleworking Policy"
3rd March 05	2.0	CRAI – ISMS Manager	SECOND RELEASE
27th September 05	2.1	Chandrashekhar Moharir – ISMS Team	Changes in software copyright compliance, Internet policy, maintaining information security, password policy.
4th Oct 06	3.0	Cmoharir- ISMS team	THIRD RELEASE
18th September 08	3.1	Dmalli- ISMS Team	Addition of acceptable use policy on Data Card / GPRS / Blackberry
19th September 09	3.1	Kamal Seepana- ISMS Team	No changes
22nd April 2010	3.2	Daksha Malli	Policy Revision
28th June 2011	3.3	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

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

			controls 5.2 and 5.7 under system password usage policy. Minor changes to section 3, 6, 7 and 8. Section 9.5 changed
15th July 2012	3.4	Manish Kamble	Addition of Client 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
17th July 2013	4.0	Sarvesh Dhuri	Minor changes in point no. 2.7 , 2.8 , 2,12 , 5.3 & Section 15

Distribution

Name	Title	Document Version	Date
Capgemini India	Acceptable IT Usage Policy_v1.0	1.0	8th Jun,2004
Capgemini India	Acceptable IT Usage Policy_v2.0	2.0	3rd Mar,2005
Capgemini India	Acceptable IT Usage Policy_v3.0	3.0	13th Nov,2006
Capgemini India	Acceptable IT Usage Policy_v3.1	3.1	18th Sept ,2008
Capgemini India	Acceptable IT Usage Policy_v3.2	3.2	20th Aug ,2010
Capgemini India	Acceptable IT Usage Policy_v3.3	3.3	15th Jul ,2011
Capgemini India	Acceptable IT Usage Policy_v3.4	3.4	28th Jul ,2012
Capgemini India	Acceptable IT Usages Policy_v4.0	4.0	05th Aug,2013

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

Reviewed & Approved By

Name	Title	Document Version	Section	Date
Mr. Amisagadda Seshaiah	AD – ITICS	ISMS-Annex-04/1.0, 1.1, 1.2, 1.3, 2.0,2.1,3.0	All	7th June 04, 10th Jan 05, 20th Jan 05, 12th March 05, 1st December 05, 16th Oct 06
Mr. Atul Srivastava	Director – PRM	1.3	All	12th March 05
Nilesh Burghate	Manager – ISMS	2.1,3.0	ALL	25th Nov 05, 9th Oct 06
Mithilesh Singh	Manager- ISMS	3.1	All	18th September 08
Sudarshan Singh	AD-ISMS	3.1	All	18th September 08
Mithilesh Singh	Information Security Officer	3.2	All	23rd September 2010
Sudarshan Singh	Head – ISMS	3.2	All	20th Aug 2010
Sudarshan Singh	Director – ISMS	3.3	All	15th Jul 2011
Sudarshan Singh	CISO	3.4	All	28th Jul 2012
Sudarshan Singh	CISO	4.0	All	05th Aug,2013

Process conformance

Standard / Model	Clause / Section / (Key) Process Area
ISO 27001:2005	Clause A.7, A.8, A.9, A.6 Control Objective A7.3, A.8.7, A.9.3, A.6.3

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

Table of content

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

1. Purpose

This policy is issued with authority of the Information Security Forum (ISF) and owned by Chief Information Security Officer (CISO) of Capgemini India. Its compliance is mandatory for all users (employees, sub-contractors, third parties) having access to any of facilities or information systems or information owned or processed by Capgemini India.
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 27001:2005.

2. Scope

This policy shall be applicable to employees, sub-contractors, third party service providers, hereafter referred as "the user". This policy shall also be applicable for users delivering services from client location and /or client provided systems and network services. In case the client security requirement supersedes Capgemini India's Acceptable IT Usage policy, the user shall follow client security requirements. In case, security requirements of the client do not meet the requirements of Capgemini India's Acceptable IT Usage Policy, explicit approval shall be taken by the project and/or the user. 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 policy framework of Capgemini India.
As stated in the ISMS Policy Manual, all references to "the company" or "Capgemini India" or "Organization" shall be deemed to refer to "Capgemini India Pvt Ltd."; it's successors in title and to any subsidiary or other organization, which it wholly or partly controls. This policy document shall be published on the Organization's Intranet or central repository accessible to all the employees of Capgemini India. 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

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

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

4.1.1 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

4.1.2 The user will be provided company assets (desktop, laptop, authentication tokens, phones etc.) and information systems or services access (internet , PSTN , VoIP , client's system , intranet etc.). The assets and services should be used for delivering services to the company and should not be used improperly. The user should ensure security of such access .Any misuse of these assets or access will be attributed to the user only.

4.1.3 The user will be provided access to its client's IT systems and services (email ,internet , business information systems etc.) .These access must be used for delivery services to the customer ; its usage must be governed by the customer's information security policy .In case of any ambiguity on such use , the user should seek clarification from its project manager or the client .

4.1.4 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", "customer confidential" and "sensitive" information.

4.1.5 The user must not send any information classified as "company confidential", "customer confidential" and "sensitive" to its personal email or must not copy these to any personal device.

4.1.6 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.

4.1.7 The user must not attempt to access a system to which one have no authorisation.

4.1.8 ISMS team has right to monitor all systems

4.1.9 Project related data must be saved on a corporate information repository (network drive on file server, share point portal, Team Forge). The only

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

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 responsible for safekeeping and security of the data stored on its laptop.

4.1.10 Only members of ITICS department are permitted 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 ITICS department (a) peripheral devices of any kind (digital cameras, PDA's, modems, etc.) and (b) removable media devices including CD writers, tape backup, floppy drives, memory sticks, flash cards, USB memory 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

4.1.11 Disposal of IT equipment shall be arranged by ITICS with due consideration of legal (software compliance) and environmental issues .No user shall dispose any IT equipment.

4.1.12 No user shall disable, circumvent or disrupt working of any security controls (Anti-malware, GPO, Patch, Encryption, web filtering etc.)

4.1.13 Capgemini India has deployed encryption solution on all of its laptops, in order to safeguard information stored on laptops. It is the user's responsibility to inform ITICS / ISMS if its laptop is not encrypted.

4.1.14 Online mass storage facility (Drop box/Sync/ Rapid Share/ Google Docs 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.

4.2 Copyright Compliance

4.2.1 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 ITICS, subject to the necessary authorization

4.2.2 The user shall not make any copies of software under any circumstances without explicit written permission of the ITICS.

4.2.3 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

4.2.4 No User shall give any organization software to any outsiders, including customers unless authorized by ITICS.

4.2.5 Any User, who determines or suspects misuse of software within the organization, shall notify IT Helpdesk and ISMS function.

4.2.6 All software must be purchased through ITICS function ,

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

4.2.7 Users are not permitted to bring software from home, and install it on to any systems of Capgemini India

4.2.8 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.

4.2.9 All software, information, programs and code developed for and/or on behalf of Capgemini India or with the use of computers and other applications which are the property of Capgemini India by employees/contractor shall remain property of or considered property of the organization or the client for whom the software was developed at the sole discretion of Capgemini India. 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.

4.2.10 Users are not allowed to install software, which are listed in Blacklisted Software (Refer latest version of Blacklisted Software)

4.2.11 No user shall install any virtual instance on any of the workstation or server without proper approval and authorization from ITICS

4.3 Clear Desk & Clear Screen

4.3.1 Each User shall maintain CLEAR DESK policy at its working place. No printed documents or soft media (CD/DVD/Floppy) classified as "company confidential ", "customer confidential" or "sensitive" shall be kept in public view or open desk while not at work. All Classified "Company confidential", "Customer confidential" or "Sensitive" papers must be shredded before disposal; classified documents including customer-supplied documents shall be kept under lock and key.

4.3.2 Computer 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.

4.4 Password

4.4.1 The user will be provided its unique system 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.

4.4.2 All project related servers including database whether in test function or production environment, shall be configured with unique user id and password.

4.4.3 Here is an illustrative list of "do's and don'ts" in dealing with password and authentication credentials

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

- Do not use the same password for internal system (domain account - Capgemini) and external system access (customer provided systems).
- 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 call the ITICS-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 , these 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 is a strong possibility that there may be KEYLOGGER or other SPYWARE programs running in stealth mode to capture your account detail and password.

4.4.4 If an account or password is suspected to have been compromised, report the incident to ISMS function (isms.in@capgemini.com or ITICS helpdesk on 7744) and immediately change all passwords

4.5 E-Mail

4.5.1 The company provides its e-mail to assist employees in the performance of their jobs. Its use shall be limited to company business. However, occasional use of e-mail for personal reasons is permitted by the organization, with the understanding that personal message will be treated the same as business messages and is subject to review.

4.5.2 Personal use of the e-mail system (web mail) should never affect the normal traffic flow of business related e-mail. Capgemini India reserves the right to purge identifiable personal e-mail to preserve the integrity of its e-mail systems. Users are allowed to access their personal emails from 1pm to 3pm and 10pm to 1am. No User shall 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;

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

- 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.

4.5.3 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.

4.5.4 The 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 ISMS .But under no circumstances; it should be forwarded to anyone inside or outside the organization.

4.5.5 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 function. Users shall ensure that all outgoing e-mail contains standard company disclaimer.

4.5.6 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.

4.5.7 Under no circumstances , user should send e-mail from a computer that where one is not logged ; impersonation shall be considered as violation of security policy

4.5.8 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.

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

4.5.9 The user shall not subscribe to e-mail lists, which are not in organization's interest

4.5.10 The user shall not subscribe to email list, where content are inappropriate and objectionable. The broad category of objectionable content is illustrated in clause 4.5.2

4.5.11 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.

4.5.12 The facility to automatically forward e-mails shall not be used to forward messages to personal e-mail accounts. Capgemini India provides a number of solutions for accessing the Capgemini India's e-mail system when away from the office.

4.6 E-MAIL – active sync configuration for smartphone and tablet

4.6.1 Only standard provision-able devices are allowed

4.6.2 Devices supporting following features shall be allowed to configure to receive email

- mandatory password with minimum length of 4 characters,
- password expiration 60 days,
- maximum 10 password attempts before phone being locked,
- automatic screen lock on 30 minutes of inactivity

4.7 Internet Usage Policy

4.7.1 Capgemini India shall provide access to internet to all users to assist them in performance of their jobs.

4.7.2 No messages will be posted on any internet message board or other similar web based service or any social networking sites that would bring the company into disrepute, or which a reasonable person would consider offensive or abusive. The list of prohibited material is the same as illustrated in section 4.5.2. 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 financial gain, nor shall user host a personal web site on any company's equipment

4.7.3 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, etc.

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

4.7.4 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 4.5.2

4.7.5 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.

4.7.6 For communication with external clients , the usage of the following Instant messaging systems are allowed:

a. Yahoo messenger

b. AOL

c. MSN

d. Web based GTALK

However file transfers and webcam facilities on these messengers are blocked. Capgemini India monitors and logs all internet accesses by individuals and reserves the right to access and report on this usages

4.8 Data backup and restore policy

4.8.1 The user is required to save all business related data on central file server. ITICS is not responsible to take any backup of data on user workstations and laptops.

4.9 Mobile & Tele-working Policy

4.9.1 The users shall ensure safety of the company assets (laptop, smartphone , authentication token) allocate to them at all times

4.9.2 Connecting to Organization's network from remote location shall only be allowed through pre-defined authentication and authorization mechanism

4.9.3 User should not attempt to dial-in or connect to Internet using data card when they are connected to Capgemini network.

4.9.4 Employee shall ensure that while accepting visitor within the company premise, they should help the visitor declare any information materials such as laptop, CD, floppy media Laptops shall not be left on the desk or in the work area overnight. Employee shall not left laptop unattended in cars, in public area like airport and hotel lounge. Laptop shall not be checked-in as baggage

4.10 Policy on Data Card / GPRS /Blackberry usage

4.10.1 Depending upon work responsibilities, the user will be provided internet connection and accessibility of office mail through data card modem or /and GPRS (General Packet Radio Service) or/and Smartphone (Blackberry) or similar technologies. The controlled use of the service or facility shall be sole

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

responsibility of the user and any liability arising due to inappropriate use will be of the user only.

4.10.2 The mobile connectivity medium (data card / GPRS / Blackberry or equivalent technology) shall be used only for legitimate business purpose.

4.10.3 The mobile internet connectivity may enable an uncontrolled access to internet. Even in such case, the employees must not publish, display, store, request (download) or transit any objectionable information

4.10.4 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 ISMS team through mail (isms.in@capgemini.com) and phone (extension: 7744).

4.11 Access to Corporate WIFI infrastructure (XS4Mobiles and XS4Guest)

4.11.1 Non-company devices may be connected to X4mobile and X4GUEST wireless profiles only.

4.11.2 Employees needing access to X4mobile shall require providing specific business justification and their line manager approval. Such access shall be enabled by specific MAC authentication mechanism.

4.11.3 Access to guest wireless network (X4Guest) shall be provided only to client and external third party (for example auditors) with business justification. The user credential (user ID and password) will be unique to the user.

4.11.4 No user shall setup wireless infrastructure or create ad-hoc network

4.12 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 reputational or information loss. The employee needs to adhere to the below guideline in using social network sites.

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

4.12.1 Publishing and social networking must be done in a professional and responsible manner.

4.12.2 Public statements about Capgemini India, Capgemini Group and Capgemini Group's vision must be approved by Corporate Communication.

4.12.3 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.

4.12.4 Employees should not identify themselves as a representative of Capgemini India.

4.12.5 Any employee representing as Company representative giving public statement about Capgemini vision must be approved by Corporate Communication.

4.12.6 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.

4.12.7 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.

4.12.8 Capgemini India or its customer's confidential or proprietary information, trade secrets or any other material covered by the Capgemini India or its customer's confidentiality information must not be revealed or discussed.

4.12.9 The user shall comply with copyright and fair use of the media

4.12.10 The user shall show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory for example politics, sexual orientation and religion, ethical, obscenity.

4.12.11 Company logos and trademarks shall not be used without written consent.

5 Reporting of security incident:

All users (employees, contractors, sub-contractors) are responsible to report any security incident to ISMS function. 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

Printed copies are current on distribution date. Always refer to the electronic version for the current release.

The security incident and/or potential security incident must be reported to ISMS function at isms.in@capgemini.com or on ITICS helpdesk at extension 7744.

Printed copies are current on distribution date. Always refer to the electronic version for the current release.