INSOLVENCY PROFESSIONAL AGENCY
OF INSTITUTE OF COST ACCOUNTANTS OF INDIA (IPA ICAI)

INFORMATION TECHNOLOGY POLICY OF INSOLVENCY PROFESSIONAL AGENCY OF INSTITUTE OF COST ACCOUNTANTS OF INDIA

VERSION 1.1

CONTENTS

1. CHARTER OF THE POLICY

1.1 CHARTER

The charter defines the followings:

- Purpose
- Scope
- Authority
- Aims and Commitments
- Constitution of the Committee
- Scope of the IT Committee

1.1.1 Purpose

The objective of the IT Policy is to provide a conformity instrument for the various functions relating to availability of hardwares/softwares/updated information on website/web applications and IT security in the organization. It provides a complete documentation of the various procedures to be followed within IT domain of IPA ICAI. The policy also serves to recognize and understand important issues and to ensure consistent thinking and action on these issues by people within IPA ICAI.

1.1.2 Scope

The scope of the IT policy framework includes all the users viz. employees/staff members (permanent, contractual, interns, trainees), other contractual/out-sourced service providers (hosting server providers, security auditors, Wi-Fi service providers, Internet Banking Facility Provider and similar), Board of Directors and other related stakeholders, as may be applicable and is hereinafter referred as Authorized Users.

The scope of the IT Policy applies to hardware assets viz. Laptops, Desktops, Chargers, Printers, Scanners, Photocopier, External Hard Disks, and any other devices as may be applicable and provided by IPA ICAI and used for the development of IPA ICAI.

The scope of the IT Policy includes internet usage, official email usage and users accessing the email services of IPA ICAI for the development and growth of the business of IPA ICAI, password protection procedures applicable to user level and system level passwords having access to the systems, official e-mail ids, Users, who have been given access for the Operations/data of IPA ICAI and also all the resources of access to internet including computer, laptop, mobile etc. belonging to IPA ICAI and/or devices owned by the employees, where such devices are being used, to access the internet resources /information assets of IPA ICAI. The scope also includes Bulk Communication in the form of SMS/bulk e-mailers/Broadcasting (WhatsApp) and other Social Media Communications platforms as approved by IPA ICAI.

The scope of the IT Policy is concerned with the management and security of the information assets of IPA ICAI (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to IPA ICAI) and the use made of these assets by its members and others who may legitimately process IPA ICAI information on behalf of IPA ICAI.

1.1.3 Authority

All information collected by means of IT data collection methodology and platforms, the sole ownership is of IPA ICAI and IPA ICAI is authorized to extract, utilize and store the information as the need be.

All embedded IT procedures and enforcement measures shall be regularly reviewed & monitored by the IT Committee (ITC). The Secretary of IT Committee shall be responsible for the administration of this Policy document in consultation with the IT Committee, IT Network & Security Audit Team, IT Web Hosting Team and IT Web Application development Team.

1.1.4 *Aims and Commitments:*

a. IPA ICAI recognises the role of information in ensuring that Authorized Users have access to the information they require in order to carry out their duties/ work. Computer and information systems underpin all the activities of IPA ICAI and are essential to its operations and administrative functions.
b. Any reduction in the confidentiality, integrity or availability of information could prevent IPA ICAI from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information might have the potential to damage the reputation of IPA ICAI and might cause financial loss.
c. To mitigate these risks, IT policy must be an integral part of information management, whether the information is held in electronic form or hard/soft copy form.
d. IPA ICAI is committed to protecting the security of its information and information systems in order to ensure but not limiting to that:
    - the integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose'.
    - information is always available to all those Authorized Users, who access to the information system of IPA ICAI, who need it and there is no disruption to the business of IPA ICAI.
    - confidentiality is not breached, so that information is accessed only by those authorised to do so;
    - IPA ICAI meets its legal requirements, including those applicable to personal data under the prevailing law, if applicable any.
    - the reputation of IPA ICAI is safeguarded.
e. In order to meet these aims, IPA ICAI is committed to implementing security controls that conform to best prevailing practice.

f. Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.
g. IPA ICAI is committed to providing sufficient education and training to authorized users to ensure that they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information.
h. Specialist advice on information security shall be made available to all with IPA ICAI.
i. An information security group (or groups) presently called as 'IT Committee', comprising representatives from IPA ICAI and the governing board, shall advise on best practices and coordinate the implementation of information security controls.
j. Breach of information security must be recorded and reported to MD/CEO/committee secretary and/or any appropriate authority of IPA ICAI, who may initiate disciplinary action(s), and inform the relevant authorities. Secretary, IT Committee, would maintain the records abiding the law (as on date it is for 8 (eight)years).
k. Deletion of any record is prohibited, without the approval of the MD/CEO which would be recorded in the record keeping register.
l. This Policy and all other supporting policy documents shall be communicated as necessary throughout IPA ICAI to meet its objectives and requirements.
m. Security Audit would be performed as per the policy.

1.4.1. Constitution of the IT Committee:

The IT Committee of IPA ICAI would be constituted by the Governing Board of IPA ICAI.

The IT Committee shall consist of at least four members as per details below, which may be extended on the recommendation of the Chairperson and approval of the Board of Directors, as per requirement:

a. An Independent Director to be the Chairperson of the Committee.
b. A person with technical knowledge.
c. Managing Director/ CEO of the IPA ICAI, as may be applicable.
d. The Secretary of the Committee would be an officer of IPA ICAI, who would be selected by the IT Committee and would be responsible to carry out the duties mentioned here further.
e. Any other member as may be recommended by the Chairperson.

1.4.2. *Scope of the IT Committee:*

The IT Committee (may be referred as ITC) should consider the matters relating to and in respect to IT periphery of IPA ICAI and make recommendations to the Governing Board for:

- ensure that users are aware of this policy,
- seek adequate resources for its implementation,
- monitor compliance,

- conduct regular reviews of the policy, having regards to any relevant changes in legislation, IBBI guidelines, organisational policies, contractual obligations and any other need as may be felt required,
- ensure there is clear direction and visible management support for security initiatives,
- ensure arrangement of training programs as and when required to all the authorized users.

1.2 CONFIDENTIALITY OF INFORMATION

IT Policy (ITP) document contains information which are deemed to be proprietary and sensitive in nature. The authorized users and IPA ICAI hold the complete responsibility to maintain the confidentiality of all the information received related to its professional members and related stakeholders through various IT platforms.

1.3 ENFORCEMENT

This Policy document is applicable to all the authorized users and related stakeholders of IPA ICAI. This policy also applies to Consultants, Advisors or any third party engaged in working along with IPA ICAI on any project or assignment related to IT.

Any Authorized User and related stakeholders found to have violated any provision(s) of this IT Policy, may be subject to fine/disciplinary action, as may be deemed fit, as per IPA ICAI norms.

1.4 WAIVER CRITERIA

This policy is intended to address IT security requirements. The requested waivers exception to Policy must be formally submitted to Secretary of IT Committee including justification and benefits attributed to the waiver. Depending on the type and impact of the waiver request, the Secretary of IT Committee would either approve or escalate to the MD/CEO/IT Committee for approval. The waiver shall only be used in exceptional situations when communicating non-compliance with the policy for a specific instance/period of time as may be specified in the request, not exceeding one calendar month. At the completion of the time period the need for the waiver shall be reassessed and re-approved, if necessary. Each such instance should be requested through a written communication in the form of e-mail or similar. Each such instance should be recorded in the Waiver Log Register to keep a track.

2. POLICY STRUCTURE

The IT Policy consists of the following parts: -

2.1 INFORMATION SECURITY
2.2 USAGE OF INTERNET FACILITY
2.3 E-MAIL HANDLING
2.4 PASSWORD PROTECTION

2.1: INFORMATION SECURITY:

This part of the IT policy provides a framework for the management of Information and Security of IPA ICAI and applies to:

a. All Authorized Users who access to information of IPA ICAI.
b. Any system(hardware/software) attached to IPA ICAI computer/ server or telephone network (including mobiles/ cell phones) and any system installed by IPA ICAI.
c. All information (data) processed by the IPA ICAI pursuant to its operational activities, any communications sent to or from IPA ICAI and any IPA ICAI information (data) held on systems external to the network of IPA ICAI.
d. All external parties that provide services to IPA ICAI in respect of information processing facilities and business activities and also the internal parties who access to the information system of IPA ICAI, including all Authorized Users.

2.2: USAGE OF INTERNET FACILITY

i. The internet resources of IPA ICAI are for the official and business use of IPA ICAI and to secure the interest, IPA ICAI may monitor these resources and as such, the Authorized Users are advised not to access or share their personal information on these resources and if they are accessing or sharing such information it shall be presumed that the same will be done at the risk of the individual user and the user cannot claim the privacy for personal sensitive information.

ii. The theft/ hacking of data always took place consequent to the compromise of authentication data and as such, it shall be the responsibility of all the Authorized Users to protect their authentication data such as user ID and Password. In the event of failure, the Authorized Users shall be liable for all such damages/ offenses which may be caused for any offence committed thereof.

iii. IPA ICAI shall make its best endeavour to inform the Authorized Users from time to time, the method or technique used by the cyber criminals to hack the data by use of phishing, sending the malware/ backdoor etc. in addition to the policy mentioned herein.

iv. All Authorized Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services as the same are contravention as well as criminal offence under Information Technology Act, 2000. Any accidental damage or disruption must be reported to IT / Line Manager as soon as possible after the incident has occurred. Authorized Users are responsible for any IT activity which is initiated under their username.

v. Use of the Internet by Authorized Users is encouraged where such use is consistent with their work and with the goals and objectives of IPA ICAI in mind.

vi. Users must not participate in any online activities that are likely to bring IPA ICAI into disrepute, create or transmit material that might be defamatory or incur liability on the part of IPA ICAI or adversely impact on the image of IPA ICAI.

vii. Authorized Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race, hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs. These are offences punishable under IT Act, 2000 & other laws. Do not visit to the sites which are having offensive material which include videos and images.

viii. Authorized Users must not knowingly introduce any form of computer virus into the computer network of IPA ICAI and same is also cyber contravention and criminal offence under IT Act, 2000.

ix. Personal use of the internet is discouraged.

x. Authorized Users must not "hack into" unauthorised areas which is a criminal offence under IT Act, 2000 and may attract disciplinary action against the concerned individual.

xi. Authorized Users must not download commercial software or any copyrighted materials belonging to third parties unless such downloads are covered or permitted under a commercial agreement or other such license or are used for value addition to IPA ICAI.

xii. Authorized Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.

xiii. Authorized Users must not use the internet to send offensive or harassing material to other users.

xiv. Set your computer to lock your screen automatically to protect sensitive data and can take the help of IT department for installing the same.

xv. Do not visit untrustworthy sites out of curiosity, or access the URLs provided in those websites. Do not download any media files from the internet like music and movies.

xvi. Do not visit the sites where there is notification from the Browser/ Firewall/ Pop-up message/ Website like it can be harmful for the system/ IT environment of IPA ICAI.

xvii. Do not access or visit the website by clicking on the hyper link in the email/ pop up messages and it is advisable to write the appropriate URL in the URL bar.

xviii. Be aware of the deceptive URL such as www.microsoft.com may be written in the link as www.micosoft.com etc.

2.3: EMAIL HANDLING

i. Office Staff shall be responsible for maintaining upkeep and integrity of all IT resources provided to them in the course of work.
ii. The official email system is intended for use in conducting business of IPA ICAI. All email messages shall be considered as record of IPA ICAI.
iii. The official email shall not be used for personal, commercial or political purposes.
iv. No messages / data of IPA ICAI shall be shared with any outside person by any individual or with any external entity, except as required in discharge of duties of IPA ICAI in conformity with the guidelines of IPA ICAI. IN case any data in specific is to be shared with any person not connected with the affairs of IPA ICAI, the same shall only be done with prior explicit approval from MD/CEO.
v. The official email shall not be utilized for storing, distributing or disseminating images, text or materials (including screen shots) that might be considered indecent, pornographic, obscene, illegal, discriminatory, offensive or abusive or might be considered as harassment or are not permitted under any law. These acts are criminal offences which are cognizable and punishable under Information Technology Act, 2000.
vi. Official email facility shall not be used for spamming, unauthorized promotions / advertisement to external world or sending / forwarding chain letters unless meant for promotional activity and business development of IPA ICAI with explicit and prior approval from MD/CEO.
vii. The communication system of IPA ICAI shall not be used for unauthorized alteration of electronic data, disruption or interference (e.g., hacking) or any other license / copyright violation.
viii. The official email service should not be manipulated including but not limited to the use of false mail header or alter the headers of mail message which disguise the identity of the sender. The act of manipulating identity is a criminal and cognizable offence under the Information Technology Act, 2000.

ix. Use of personal email account for sending official mails and other official communication is prohibited.
x. All official mails must have relevant subject matter in a precise and structured manner without including the internet abbreviations and characters such as smiley.
xi. Transmission of unsolicited commercial / advertising material or unsolicited personal views on social, political, religious or other non-business-related matters is prohibited.
xii. When sending emails to multiple recipients is unavoidable, adequate care shall be taken to remove attachments, if any, before forwarding emails to others unless they are genuinely required and use of "reply to all" function shall be avoided where information is required by only one person in the group.
xiii. Letter bombing' (sending the same mail repeatedly to one or more recipients) should be avoided.
xiv. All e-mail users shall not break into the IPA ICAI's or another Organization's system or use a password / mailbox in an unauthorized manner or unlawful manner.
xv. All e-mail users shall not directly or indirectly introduce any form of computer virus or malware into the network of IPA ICAI. Opening of emails from unknown sources should be completely avoided, and if unavoidable, then special care has to be taken while opening such emails (like ensuring latest antivirus patch availability).
xvi. The act of sending virus or malware is a criminal offence which is cognizable and punishable under Information Technology Act, 2000. In the event any malfunctioning of PCs or any spam mails are observed by the employees, they must immediately inform their IT helpdesk.
xvii. All e-mail users shall not circumvent or attempt to circumvent the prescribed network security measures including use of external storage drives, mobile scanners, etc.
xviii. All users shall abide by the above and any other guidelines or changes in law that comes into effect from time to time.

2.3.1: Email Account Management

i. To ensure security of email system, passwords for email account will have to be changed every 30 days (at least one day in advance) in terms of password protection procedure.
ii. Authorized Users must not download the attachment of the email coming in spam box.
iii. Email access management should be followed according to the under detailed chart:

Access Management Chart:

S. No.	Information Confidentiality Level	First Level Access	Second Level Access
1.	Low Confidentiality	Executives/ Assistant Mangers	MD/CEO/Secretary of the Committee

2.	Medium Confidentiality	Mid-Level Executives/Secretaries of the Committee	MD/CEO/ Secretaries of the Committee
3.	High Confidentiality	Secretary to the Committee	MD/CEO

2.4: PASSWORD PROTECTION

The Best Practices of Password protection would be applicable for all platforms/applications/device access which needs a password key for access.

i. The minimum length of passwords must be set as 8 alphanumeric characters including Upper Case, Lower-Case letter, Numeric and minimum One Special Character.
ii. Password should not be of their login ID, Employee Number, Company Name, Birthday, Address and Phone Number and Geographic Location.
iii. Password should not be preserved into any electronic communication like email, mobile or other form of electronic communication.
iv. Do not write password near your computer or on your table, walls etc.
v. Do not use the password remember option of the Web Browser like Chrome, always select the never option.
vi. Do not share the password with anyone as the user would continue to be liable for all the action taken using the password of the user.
vii. Do not steal the password of another person by any means such as shoulder surfing, key logger etc. as it is a criminal and cognizable offence. Similarly, using the password of another person is an act of identity theft under the Information Technology Act, 2000.
viii. Do not use the same password on multiple accounts as theft of password from one account would result into compromise of all accounts.
ix. Any user being suspect of that his/her password has been compromised should inform the authority and immediately change his/her password.
x. The Authorized Users to change their passwords of their accounts after each 30 days.
xi. The system must force the user to change the password at the time of the initial logon.
xii. User Ids must be locked after 3 incorrect password attempts for all critical applications.
xiii. Default passwords, of all systems or applications must be changed.
xiv. All Authorized Users must be made to sign an undertaking to keep passwords confidential and acknowledge liability for transactions done using their user IDs.
xv. Passwords must never be displayed in clear text or stored in readable form in batch files in automatic login scripts or in other locations.
xvi. Exceptions to the password management policies may be granted for certain legacy applications based on proper approval by the MD/CEO/Appropriate Authority.

2.5: BULK COMMUNICATION

i. The data received from the professional members shall be maintained and updated on regular basis.
ii. Since data is received from the professional members in confidence, it shall be ensured that the information contained in the data and the data itself so received is kept confidential.
iii. The information contained in the data or data itself shall not be shared, at any time, with any external/internal entity or any third party other than IPA ICAI.
iv. The IPA ICAI shall use data only for services like bulk email, SMS and broadcasting (WhatsApp) and other approved social media facility as provided by the IT Team of ICAI.
v. The IPA ICAI shall take all measures to ensure the security of information contained in the data or the data itself.
vi. The request for the services like SMS, Broadcasting (WhatsApp) and Bulk Mail must be made e-mails only and the request must be made at least three days before the programme by MD/CEO as may be applicable. This facility is available only for Professional Development Initiatives.
vii. The running cost of the SMS facility will be borne by IPA ICAI.
viii. The IPA ICAI shall not be liable for misuse of data or the information contained therein, such misuse occurs due to hacking or any other unlawful means. However, IPA ICAI shall be free to initiate legal proceedings in the case of hacking or unlawful use of the information contained in the data or data itself.
ix. Mails shall be deleted only with the approval of MD/CEO after citing justified reasons for deletion. The instance to be recorded in the record keeper/register.

2.6: VIDEO CONFERENCING PROTOCOLS

i. ***Platform to be used for Video Conferencing***: The IPA ICAI may decide to choose the kind of platform viz. Zoom, Team Viewer, Google Meet, Jio Meet, Skype, WebEx etc. as per qualitative and commercial consideration and approval from the MD/CEO/appropriate authority.

ii. ***Holder of the Video Conferencing ID:*** The Video Conferencing Id can be a common id being used across all departments as per requirement and after coordination with all the departments to avoid overlapping. Simultaneously, separate ids may also be created/purchased for each department.

iii. ***Creation of the Video Conferencing Link:*** In case of a common id for Video Conferencing the Admin Department should hold the password for access of the Video Conferencing platform ID. S/he would be responsible for creation of the Video Conferencing Meeting ID and share the details to the concerned department Secretary for further use, as required. In case of separate Video Conferencing ids for each department, the Secretary of the Committee is to hold the Id credentials and do the link creation and communication as may be required.

iv. ***Host/Co-host and Screen Sharing Protocol:*** The Host, by default would be the Secretary of the Committee. In case of professional development program any Office Staff assigned and

approved by MD/CEO/appropriate authority can be the Host. Permission for recording of the event should be taken from the appropriate authority. The Host, by default, displays any document to be shared on screen. In case of any requirement for displaying any document by some other participant in the Video Conference, the same may be allowed with instant/prior permissions from appropriate authority.

v. ***Saving of the Recordings of the Meeting:*** All the recordings to be done in the cloud of the meeting platform. The same, in case required, may be downloaded from the cloud/G-suite Vault with approval from appropriate authority with its record in the register.

2.6.1. Guidelines for Participants:

The Notice of the program should convey the following for the participants:

i. The participants should join the meeting at least 10 minutes before the scheduled time.
ii. The microphones should not be handled/touched to avoid sound disturbances and should be kept in mute until required and focus should be on camera while speaking.
iii. The focus should be on Camera while speaking.
iv. Background views, phone calls, eating and drinking should be avoided.
v. False impression of taking notes while in conference/ meeting should not be created by typing on the laptop keyboard or scribbling on the paper and doing personal work, while switching on the camera during meeting/conference.
vi. While participation one should be properly equipped with infra supports viz. Laptop/internet connection/bandwidth/ power supply.
vii. Personal Level recording of program is prohibited.
viii. Proper Roll calls/Attendance to be taken in a time bound manner and admission to the Video Conference after that timeline should be prohibited.
ix. In case of Committee Meetings, confidentiality must be maintained, and oath should be taken about the confidentiality.
x. Any sharing/usage of objectionable videos/unparliamentary language will call for a disciplinary action.

2.7 STORAGE & DISASTER MANAGEMENT

2.7.1. *Backup and Storage*

IPA ICAI ensures that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken regularly and timely. After each back up, a register to be maintained being counter signed by Secretary- IT Committee and MD/CEO as an evidence of Backup being created.

2.7.2 *Cloud/G-Suite Vault Backup*

IPA ICAI to have a dedicated cloud back-up/G Suite Vault system which would have the facility for auto saving, storing, non-deletion and securing the data.

The retrieval of data from the cloud/G Suite Vault should be password enabled. The backup should be real time enabled.

2.7.3. *External Hard Disks*

i. All departments of IPA ICAI are being provided with dedicated external Hard disks, which would be storing information and data for backup.

ii. The backup to these external hard disks is to be done on a weekly basis, with the backup date being recorded in a register.

iii. The Hard disks should be password protected and during each instance the Secretary of the Committee/MD/CEO would key in the password and allow the access for adding or deleting files.

iv. In case of each instance of deletion, permission/approval from the Secretary of the Committee/MD/CEO has to be taken and recorded mentioning the purpose of deletion.

2.7.4. *Any Other External Storage Device*

IPA ICAI reserves the rights of using any other external storage devices viz. pen drives, CDs, DVDs, any other form of USB ports. In case of any such requirement/exigency the employee may put a written request with detailed mentioning of the purpose and upon approval the use of such device may be allowed to be used with record on what is loaded/saved in it**.**

2.7.5. *The storage of the external storage devices*

Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers or cabinets. Where this is not practicable, and the information is kept on open shelving, the room should be locked when unoccupied for any significant length of time.

Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

Keys to be kept with the MD/CEO/ Authorized persons'.

2.7.6. *Deletion*

Confidential information/any IT Record should not be deleted without the permission of the MD/CEO/Appropriate Authority and should be properly recorded.

2.7.7. *Disposal of Secondary Storage Devices*

A separate storage box may be maintained wherein the defective/corrupted external devices may be kept within the office premises to avoid any wrong dispersal of the defective devices. The same may be kept/ disposed of with proper maintenance of the records.

Any loss or unauthorised disclosure must be promptly reported to be reported to the appropriate authorities.

2.7.8. Protection and Confidential Information

2.7.8.1. ***Access***

i. Confidential information can only be accessed by the authorised persons.

ii. All users would access through passwords. Users must follow password guidelines as designed, update, store the password.

iii. As a requirement of legislation and to allow for potential investigation, access records should be kept for a period as prescribed by regulators and tax Authorities and applicable legislations.

iv. Users with access to confidential information should be security vetted, as appropriate, in accordance with existing policies.

v. Physical access should be monitored, and access records maintained and recorded in the register for access.

2.7.8.2. *Copying*

i. The number of copies made of confidential information, whether on portable devices or media or other devices (personal/official), should be the minimum required and as per approval from MD/CEO/Appropriate Authority, and, where necessary, a record be kept of their distribution. When no longer needed, the copy should be returned to the authority or, with a record of the event in the record keeper/register being signed by the action initiator and approver.

ii. All copies should be secured by the holder of the information.

2.8: WEBSITE & ELECTRONIC FUND TRANSFERS

2.8.1. Management of Website:

i. Maintenance of the website of IPA ICAI contains:
   a. Hosting of Website
   b. Module Development
   c. Login Creation
   d. Data Management
   e. Upgradation of the Website, etc.

ii. The service of hosting of the website is done by an outsourced vendor.

iii. The other services of module development, Login creation, Data Management, upgradation of the website etc. is done by the parent institute, The Institute of Cost Accountants of India (ICAI) or any other service provider as per recommendation of the IT Committee and approval of the Governing Board of IPA ICAI.

iv. The backup of the information stored on the website is to be taken in real time mode with auto saving procedure to the dedicated cloud/server space/G Suite Vault of IPA ICAI.

2.8.2. Information on Website:

The information is collected as per the laid-out guidelines of IBBI and any changes would be done on the basis of the directions of IBBI.

2.8.3. Electronic Fund Transfer (EFT):

i. Financial Transactions take place through the website and EFT mode also.
ii. All EFT payments and receipts is done in compliance to all the financial policies of the applicable regulations of the regulators and RBI.
iii. EFT transactions have specific authorization whose passwords/one-time passwords (OTP) is with the MD/CEO of IPA ICAI.

2.9. RISK ASSESSMENT, CLASSIFICATION AND PROTECTION OF INFORMATION SYTEMS

2.9.1. Risk assessment of information held:

i. The degree of confidentiality required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.
ii. The risk assessment should identify the information assets of IPA ICAI; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to IPA ICAI. In assessing risk, IPA ICAI should consider the value of the asset, the threats to that asset and its vulnerability.
iii. Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.
iv. Rules for the acceptable use of information assets should be identified, documented and implemented.
v. Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the infrastructure, systems and processes of IPA ICAI.
vi. Professional Members data must be stored and protected in accordance with the data storage management guidelines of IPA ICAI. (website security)
vii. Appropriate technical and organisational measures be taken against unauthorised or unlawful processing of professional members/IPA ICAI's data and against accidental loss or destruction of, or damage to, personal data. (website security)

2.9.2. Protection of Information Systems & Assets and Security Audit:

i. Understanding the importance of risk assessment IPA ICAI has drawn up their own IT policy, setting out appropriate controls and procedures. Authorized Users must be satisfied that the controls will reduce any residual risk to an acceptable level.
ii. Confidential information should be handled in accordance with the requirements and according to the following chart of access control as is mentioned in the **Access Management Chart** under e-mail management segment.

iii. Security Audit by approved agencies to be conducted by IPA ICAI for the infrastructure, hardware and the software applications to be organized in span of every two years or as per IBBI guidelines.
iv. Internal Security Audit to be conducted by IPA ICAI each year for infrastructure, hardware and software applications in accordance with the prescribed format. **(Annexure I).**

2.9.3. Authentication of information through Digital Signature/e-Signature:
IPA ICAI allows Authorized Users to apply digital signature for verification/submission of the records.

2.10. POLICY COMPLIANCE

2.10.1. Compliance Measurement

The Information Technology (IT) Department will be verifying the enforcement of the policy with not limited to stated method like (sub points of the policy to be added) Periodic Checks, Internal and External audits.

The External Audits would be as per the parameters advised by Insolvency and Bankruptcy Board of India (IBBI) security audit procedures. The MD/CEO would also inspect and make sure the adherence of the policy on regular basis.

2.10.2. Non-Compliance- Violation

i. All Authorized Users/stakeholders of IPA ICAI are strictly directed to follow the policy.
ii. Anyone found violating the policy would be attracting a disciplinary action or any other penalty/punishment, as to the nature of offence/ violation and as deemed fit by the IT Committee/appropriate authority, and
iii. If such violation results in any loss of information, sensitive data, the Authorised User may also be liable to pay for such damages caused to the IPA ICAI or any third party.
iv. All official emails are subject to audit which shall be carried out by the order of MD/CEO/Appropriate Authority.
v. Non-compliance with the above guidelines shall be considered as violation of the Policy of IPA ICAI and shall be subject to appropriate disciplinary action.

2.11. HAND OVER PROCEDURE

i. The Authorized User while getting separated from IPA ICAI, would systematically and properly handover all the assets in the form of physical/ intellectual/encrypted to the immediate reporting head/Secretary of the Committee/MD/CEO, as the case may be applicable.
ii. The Authorized User is liable to handover all the passwords of email id(s), social media handles (if any), Wi-Fi or network access to the immediate reporting head//Secretary of the Committee/MD/CEO, as the case may be applicable.

iii. The Authorized User is liable to handover all the files, folders, drives, storage devices containing records/information/data pertaining to the department handled by the employee in physical or soft forms to the immediate reporting head//Secretary of the Committee/MD/CEO, as the case may be applicable.

iv. The Authorized User is liable to handover all the hardware equipments viz. laptop, desktop, external hard disks, pen drives, any other storage devices, mouse, chargers and other associated equipments, if any, in safe and sound manner to the immediate reporting head//Secretary of the Committee/MD/CEO, as the case may be applicable.

v. The to the immediate reporting head/Secretary of the Committee/MD/CEO, as the case may be applicable should refer to Admin Department to ascertain the list of assets issued and received of the respective staff and give a clearance to complete the handover procedure.

2.12. IMPLEMENTATION AND INTERPRETATION OF POLICY

i. This Policy shall come into effect from the date of the approval of the Policy by the Governing Board of IPA ICAI and shall continue to remain effective until otherwise modified or rescinded in writing by the issuer of this Policy.

ii. The IT Committee with the approval of the Board of Directors, reserves the right to add, delete or modify any clause or any part thereof of this Policy as and when it deems fit; without assigning any reason whatsoever.

iii. In case of any clarification in respect of the policy, the decision of Governing Board shall be final.

iv. Governing Board and IT Committee reserve the right to interpret the meaning of this Policy and / or any part thereof and such interpretation shall be final and binding.

3. POLICY CHANGE MANAGEMENT

The Secretary of the IT Committee is responsible for administering the information policies. This will also include updating the IT manual from time to time to incorporate updates, amendments and circumstances requiring change in policies, and training the personnel based on the inputs received from the Security Audit (Internal/External), the policy would be revised. The Secretary of IT Committee shall submit the proposal to the IT Committee for review and recommendation, before placing it to the Board of Directors for approval.

Manual's amendment history shall be maintained through "Manual Change Control Form" (MCCF).

S. No.	Activity	Prepared		Recommended by		Approved by	
		By	Date	By	Date	By	Date
1.	IT Policy	IT Committee	22nd March,	IT Committee	24th March,	BOD	25th March,

		Secretary	2021	Chairperson	2021		2021