INSTITUTE OF INSOLVENCY PROFESSIONALS

A wholly owned subsidiary of ICSI and registered with IBBI

Data Retention and Management Policy

Issued on: 23/09/2020

Approved by: Governing Board

Date of Approval: 23/09/2020

CONTENT

1. INTRODUCTION

In the course of carrying out our various organisational activities, we collect information from a wide range of sources and generate a substantial volume of data that is retained as physical records and/or electronic records. Appropriate retention of data is necessary for our operational performances and in some cases is required to fulfil statutory or other regulatory requirements and to evidence events and agreements in disputes.

However, retention of data can lead to unnecessary and excessive use of electronic or physical storage space. It is therefore essential that ICSI IIP has appropriate systems and processes in place for the preservation and timely disposal of documents and records in-line with business requirements and relevant legislation.

2. PURPOSE

This policy sets out ICSI IIP's approach for managing its information to ensure that records and documents are preserved in line with organisation's activities and legislative requirements and that data/records are not retained for any longer than necessary.

The purpose of this policy is to demonstrate/guide and provide direction on the preservation and management of information and records pertaining to various functions of ICSI IIP. This policy is also for the purpose of aiding employees in order to understand their obligations in retaining electronic documents - including e-mail, Web files, text files, PDF documents and other physical records.

3. SCOPE

This Policy specifically applies to:

- All staff, consultants, contractors, board of directors and as appropriate, partnership organisations, freelancers and third parties of ICSI IIP who maintain, process or have access to the Data;
- All records that are created, handled, stored or processed by ICSI IIP electronically (soft copy) or in physical (hard copy) form.

All those people or groups to whom this policy applies should be aware of this policy.

4. GENERAL STATEMENT

- Except as otherwise indicated, documents shall be retained for the number of years indicated in Schedule.

- First is to maintain complete, accurate and high-quality records in storage for the duration of the time periods provided for in this policy. Once any such time period is complete, the records are to be destroyed.

5. DATA STORAGE

The rules of data storage vary according to the format of data record, as set out below:

5.1 Electronic Records Storage- Documents, Email, Multimedia

All electronic documents, emails and multimedia records must be stored within the appropriate repository to ensure that applicable security, backup, retention and disposal controls can be applied. The individual who creates a record is responsible for ensuring that it is stored in appropriate location.

5.2 Physical Records Storage

Physical records that are required for the day-to-day running of business operations must be stored when not in use in the designated cupboards, filing cabinets and pedestals (desk drawers) that have been provided by Property & Facilities Management. All storage units that contain personal and confidential data records must be locked at the end of the working day. All physical special category personal data records must be stored in an appropriate filing system when not in use and these must also always be locked at the end of the working day.

6. DATA ARCHIVING

The rules on data archiving vary according to the format of a data record, as set out below.

6.1 Automated Electronic Records Archive - Documents, Email, Multimedia

Non-statutory electronic records stored on the shared drives that have not been accessed for 2 years will be automatically transferred to an electronic archive. Statutory records will be excluded from this process if they are stored in the designated departmental statutory records folder. Archived files may be accessed in read-only format through the Archive (R:\) drive until they are subsequently removed from the system, 7 years after their creation.

6.2 Physical Records Archive

Physical statutory records which are older than 2 years and don't need to be accessed on a day-to-day basis must be archived. The records will be archived either by being kept separately at the office or offsite using the document archiving service provided by Property & Facilities Management.

7. DATA RETENTION & DISPOSAL

The rules on data retention and disposal varies according to the format of a data record and the classification of the data contained within it (i.e. personal, special category personal or confidential data), as set out below.

7.1 Electronic Records Retention & Disposal - Documents, Email, Multimedia

The following retention rules apply to all Plan UK electronic documents, email and multimedia.

Non-Statutory Records: Schedule A to E

Sch.	Description	Status	Archive & Disposal Policy
A	Non-statutory shared & personal drive data	Live	Automatically archived if not accessed for 2 years
B	Archive Data	Archive	Automatically disposed of 7 years after it was originally created
C	Email Data	Live	Mailbox items automatically disposed of 3 years after they were created, sent or received. All sent and received mailbox items also logged and archived separately for 5 years.
			Deleted Items folder contents automatically cleared after 30 days.
		Archive	Mailbox items automatically disposed from the archive 5 years after they were sent or received
D	Multimedia Data	Live	Automatically disposed of 3 years after it was created (unless flagged otherwise by the Head of Department)

Statutory Records- Schedules E&F

Sch.	Description	Status	Archive & Disposal Policy
E	Statutory Documents	Live	Manually disposed of by responsible

F	Statutory Emails	Live	head of department in accordance with the retention rules.

7.2 Physical Records Retention & Disposal Schedule

No physical record will be entered into either onsite or offsite archiving without a disposal date. The retention rules that apply to physical statutory documents are outlined in Para 10

8. ELECTRONIC RECORDS BACKUP

The data and systems will have backup to protect ICSI IIP from the consequences of data loss, security breaches, system failures and disasters. The electronic records will be backed up by the IT department and shall be stored remotely as per IT services plan. The Backup frequency of all electronic records shall be monthly. Monthly backups of electronic records shall be maintained by IT department of ICSI IIP.

9. MEMBER'S DATA PROTECTION

ICSI IIP collects the personal information of Insolvency Professionals during registration and enrolment with the institute. This personal information includes person's name, email addresses, telephone number, Residence Address etc., that are collected and used for the purpose of granting membership. This personal data of members may be used i.e. in legal sense, 'transferred' and 'processed' in and outside the organisation. ICSI IIP is responsible for protection of Personal Data of its registered IPs. The personal data of registered IPs will not be made available in public domain on the website of ICSI IIP. Only authorised persons with the credentials of login ID and password may access the members' details.

10. SECURITY MEASURES AND SYSTEM AUDIT

System measures refer to protecting the data from theft, unauthorized access and modifications, and accidental or unintentional damage. In computerized systems, security involves protecting all the parts of computer system which includes data, software, and hardware. Systems security includes system privacy and system integrity.

- **System privacy** deals with protecting individuals systems from being accessed and used without the permission/knowledge of the concerned individuals.
- **System integrity** is concerned with the quality and reliability of raw as well as processed data in the system.

At the direction of Governing Board, System Audit will be carried out annually to do detailed tracing of effective internal control system in protection of data of organization. In this phase, the system auditor will comprehend the management practices and various functions used at multiple levels, crucial weakness to be identified in data retention and

protection. The main aim of the audit is to check for vulnerabilities and loopholes in the system and how the productivity, efficiency, and efficacy of the system can be improved.

11. RISK MITIGATION & DISASTER MANAGEMENT

There are several categories of disasters that might impact data of the organization such as natural disasters, technology malfunctions, Cyber Security Threats, human error, and malicious intent

Following measures to be followed for risk mitigation and Disaster Management−

(i) Backup

- Regular backup of databases daily/weekly depending on the time criticality and size.
- Incremental back up at shorter intervals.
- Backup copies kept in safe remote location particularly necessary for disaster recovery.
- Duplicate systems run and all transactions mirrored if it is a very critical system and cannot tolerate any disruption before storing in disk.

(ii) Physical Access Control to Facilities

- Physical locks and Biometric authentication.
- ID cards or entry passes being checked by security staff.
- Identification of all persons who read or modify data and logging it in a file.

(iii) Using Logical or Software Control

- Password system.
- Encrypting sensitive data/programs.
- Training employees on data care/handling and security.
- Antivirus software and Firewall protection while connected to internet.

(iv) Disaster Recovery Plan

- Define Criticality
- Define recovery objectives
- Decide on the right and updated tools
- Document and communicate recovery plan
- Test and practice the disaster recovery plan
- Evaluate and update disaster recovery plan on time to time basis
- Set up a functional team

12. OTHER GUIDELINES FOR DATA PROTECTION

a) The incorporation documents of the company will be kept in the safe custody of the Company Secretary(CS) of the company. Access to those documents is restricted to the Office in charge and the executive dealing with them.

b) Documents related to appointment/reappointment and retirement of directors on the Governing Board of the company and various committees: After every change in the composition of the Board and committees, the relevant documents are duly filed with ROC, the records are signed approved and kept in physical and electronic mode under safe custody of the CS of the company. Access to these documents will be restricted for only statutory requirements (inspection and Annual filing), that with the approval of CS of the company.

c) Documents related to meeting of Board and Committees: The notice and agenda of the meetings will be sent to the members through physical and/or email as per the requirement. The drafting of notice and agenda will be carried out by the secretariat and is supervised by the CS.

d) Membership Records: Upon enrollment of a person as Insolvency Professional (IP), physical file is created along with an electronic record of the same which is saved on the server. For the purpose of PREC and registration with IBBI, details of the concerned person will be forwarded to the Training Dept. Upon registration with IBBI as an IP, the files will be stored with the database where the existing data of IPs are maintained. Access to the storage will be restricted and can be accessed only after making entry in the log book which will be maintained by the executive/assistant handling membership database. Online database can be accessed by only by the membership department with the HOD's approval.

e) The membership records will be extracted upon events like – annual Inspection by IBBI, receipt of complaint against an IP, disciplinary proceedings initiated against an IP, etc. So, currently the credentials of IPs will be saved at three locations:

   i. Website (contact and basic details like work ex and qualifications)
   ii. Physical files which will be stored at the file storage facility
   iii. Electronic folders which will be saved on the server

f) Monitoring Records: The data pertaining to monitoring functions will be obtained through the dedicated email ids and monitoring portal of company's website. In cases, where the data will be provided by IPs on IBBI's website, records will be compiled. On the basis of that, the records will be processed and stored for further actions like follow up with the IP regarding assignments handled or initiating inspections of the IP. Considering the sensitivity of the data, access to the

monitoring records will be limited to the executives accessing those portals/email ids and folders.

g) Inspection Records: Prior to inspection, the order and notice will be issued by the company to the concerned IP. The inspection notice will be issued in electronic as well as physical form. Prior communication with the IP will be made and required Pre Inspection Questionnaire will be sent and desktop monitoring will be carried out. During the Inspection physical verification of records is carried out along with compliance of Code and Reg. is ensured. Interim Inspection Report will be submitted to the Managing Director by the HOD of monitoring deptt. Upon approval of the MD, the Final Inspection Report is placed before monitoring committee for further actions (if any).

h) Complaints and Grievances Records: Upon receipt of allegations and complaints against an IP, a physical file will be created which contains all the allegations and complaints received regarding the concerned IP, a scanned copy is also kept in case the complaint has been lodged only through physical files. Considering the sensitivity of the allegations and complaints, this process will be carried out with the legal and monitoring departments under the guidance of their HODs. The grievances will be put forwarded to the GRC for their opinion and upon their recommendation it is processed further.

i) Document Protection Documents (hardcopy, online or other media) will be stored in a protected environment for the duration of the Document Retention Schedule. Computer backup media will be included.

j) Document Destruction Hardcopy of documents will be destroyed by shredding or fire after they have been retained until the end of the Document Retention Schedule. Copies of computer backups will be destroyed by fire or other proven means to destroy such media after they have been retained until the end of the Document Retention Schedule.

13. RECORDS RETENTION & DISPOSAL SCHEDULE:

In order to facilitate, a **Record Retention & Disposal Schedule** is prepared as follows:

Area	**Record**	**Disposal Policy**	**Accountable Head**
Corporate Records	Records on establishment and development of the organisation's legal framework and governance	8 years after end of life of organisation	Secretariat
	Boards papers and minutes	8 years after end of life of organisation	Secretariat

	Management papers and minutes	8 years after end of financial year	Secretariat
	Litigation/legal papers	8 years after settlement of case	Legal
	Strategic plan, business plan, risk plans	8 years from completion	Secretariat
Finance	Financial records	8 years after date of signing of accounts	Finance
	Property acquisition (purchase, donation, rental, transfer) Deeds and certificates	8 years after end of ownership/asset liability period	Finance
	Property leases	15 years after expiry	Finance
	General contracts and agreements	8 years after contract termination	Finance
	Invoices and Bills	8 years	Finance
	Audit Reports	8 years from completion	Finance
	Income tax returns and filings	8 years	Finance
Human Resource Management	Job applications and interview records for unsuccessful applicants	12 months after interview	HR
	Payroll records – salaries and other payments through payroll	6 years	HR
	Payroll records - Maternity, Paternity, Adoption records	3 years after end of the year	HR
	Pension details - name, National Insurance number, opt-in notice and joining notice.	6 years after effective date	HR

	A summary of record of service e.g. name, position, dates of employment, pay	6 years after end of employment and permanently in electronic form	HR
	Timesheets, pay records and supporting documents such as contracts and contractual letters for employees charged to awards	6 years after end of employment	HR
	All other HR documents	1 year after end of employment	HR
Insolvency Professionals Records	Training Records (CPE/PREC etc.)	Permanently	Monitoring & Membership
	Enrolment Records	8 years after surrender of membership	Monitoring & Membership
	Assignments Records	12 years of completion of assignments	Monitoring & Membership
	Monitoring Records	Permanently (in electronic form)	Monitoring & Membership
	Inspection Records:		
	(a) Inspection Reports (Interim/Draft/Final)	5 years in case of dispute, the report shall be preserved till the resolution of dispute or 5 years, whichever is later.	Monitoring & Membership
	(b) Other records/Working papers	2 years: from the date of submission of final inspection report.	Monitoring & Membership
	Grievances Records	8 years-physical and permanently in electronic form	Monitoring & Membership

The disposal schedule will be as per the above table, however the same may be reviewed as per applicable regulations from time to time or specified circumstances by the legal department of ICSI IIP.

14. REVIEW OF THE POLICY

The implementation of the Policy will be monitored and reviewed by the Governing Board as and when required.

15. CONCLUSION

Compliance with this policy is the responsibility of each departmental head with all its vertical staff jointly / severally responsible. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Head of the Department and if necessary with the Head of IT. The staff will be educated/guided periodically on data protection and security by the compliance department on ICSI IIP.

****