

CATEGORY	Description	Sample Documents/Records	Physical and Administrative Controls	Reproduction	Distribution	Retention	Destruction/Disposal
Public	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders. A Director must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organization.	Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices	Author/Asset Owner: responsible for assessing confidentiality category and implementing any marking requirements.	Unlimited	No restrictions	No restrictions	Recycling/trash
Internal	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient. Disclosure to anyone outside of The Software Bureau requires Director level approval.	Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorized release), investment options, transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages	Author/Asset Owner: responsible for assessing confidentiality category and implementing any marking requirements. User: responsible for proper storage and document control.	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.	Internal: use a sealed envelope. External: use a sealed envelope. Electronic: use Teams, OneDrive/SharePoint, and internal email system. Encryption is required for transmission to external email addresses.	No restrictions	Paper documents: shred. Electronic data: erase media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal
Proprietary	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager.	Cygnus Source code. Swift Source code. SwiftCore Source code. Business plans.	Author/Asset Owner: responsible for assessing confidentiality category and implementing any marking requirements.	Copies may be made only by permission of originator or his/her designates or with direct authority of an appropriate director. An Audit trail must be maintained (such as an email message trail).	Electronic: Encryption is required for transmission outside the office such as staff VPN links, https and ssl. Any portable devices must be encrypted	No restrictions	Paper documents: shred using an approved cross-cut shredder. Electronic data: erase media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.
Internal Confidential		Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, other highly sensitive or valuable proprietary information	Originator: responsible for ensuring that confidential information is distributed on a strict need-to-know basis. Recipient: responsible for ensuring that confidential information is encrypted and secure when not in use.		Internal: use a sealed envelope. Hand deliver if possible. External: use a plain sealed envelope. Hand deliver or send by registered mail, courier etc . Electronic: use Teams personal messaging, OneDrive/SharePoint, and internal email system or via an Encrypted data link such as ssl or https.	See Record Retention Policies	
Industry Confidential	Highly sensitive customer provided data. Must only be disclosed to previously authorised 3rd parties, this requires the explicit permission of a Director-level senior manager.	Industry/Customer provided data	Author/Asset Owner: responsible for assessing confidentiality category and implementing any marking requirements. Originator: responsible for ensuring that confidential information is distributed solely on contractual obligations. Recipient: responsible for ensuring that confidential information is encrypted and secure.	None outside contractual obligations or without the direct authority of the 3rd party.	Electronic: encrypted data link such as ssl or https for contractual obligations only. No other distribution without the direct authority of the 3rd party.	On job completion NONE - Unless under a specific contractual agreement. Further details re. Job logs and set up are contained in the linked Record Retention Policies sheet.	Electronic data: erase media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.

This work is copyright and based on an original work by Richard O. Regalado and ISO27k implementers' forum, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum www.iso27001security.com, and (c) derivative works are shared under the same terms as this.

Data Type	Type of Record	Retention Period	Reason for Length of Period
Personnel	Personnel files including training records and notes of disciplinary and grievance hearings	6 years	Statute of Limitations
	Application forms/interview notes	At least 6 months from the date of the job advertisement	Time limits on litigation
	Facts relating to redundancies where less	6 years from the date of redundancy	As above
	Facts relating to redundancies	12 years from the date of the redundancies	Limitation Act 1980
	Income Tax and NI Returns, including	6 years	Statute of Limitations
	Statutory Maternity and adoption Pay	6 years	Statute of Limitations
	Statutory Sick Pay records and calculations	6 years	Statute of Limitations
	Wages and salary records	6 years	Taxes Management Act 1970
	Individual pension entitlement and contribution history	As long as there is a member or dependant liability	Pensions Act 2008
	Accident books, and records and reports of accidents	6 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
	Health Records	During employment	Management of Health and Safety at Work Regulations
	Health Records where reason for termination of employment is connected with health, including stress related illness	6 years	Statute of Limitations
	Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
	ISMS Documentation	Common Sense	As required for retention of evidence for auditing

Data Type	Type of Record		Retention Period	Reason for Length of Period
Customer	Correspondence		At least 6 years from the date that the customer ceases to trade with The Software Bureau, in case of litigation.	Limitation period for negligence.
	Job details and records		2 years	Reasonable period to cater for customer enquiries.
	Data	Suppression Lists	"Delta" - incremental - releases and indices are held onto as long as is required to allow us to build full builds of suppression lists Source data is removed within 30 days from receipt	Requirements of the Suppression List build process
		Bureau Jobs	At the end of every month any bureau job older than 2 months is archived. Any archived jobs older than 3 months are deleted completely.	Allowing reasonable time for responding to complaints
		Support Queries	None once specific job is completed unless specified under contract.	Data Protection Act.
		SwiftCore/ Clean Contacts	Cloud based service, all data is automatically encrypted, anonymised and deleted. No data retention once processed	Highest level of security and customer confidence.
		CIP	Client Address Data – 45 days auto cull (Time to Live in Cosmos DB) Meta Data – hold on to it for 12 months for analysis purposes Downloaded data is to be treated as Test Data CIP data is single PII (just address) Refer to "CIP DPIA v2.docx" for more detail	Highest level of security and customer confidence.
		SFTP Data	Data uploaded by clients to our SFTP can be remotely deleted by the client if they wish. Otherwise all content is automatically deleted once it reaches 31 days in age.	Allowing reasonable time for reference to supplied files for both client and ourselves
		Test Data	Unless data reflects a suppression list, then test data should always be pseudonymised using SafeData or by removal of unnecessary details (e.g. Name elements) In both cases the data will never require destruction. Test data can be included in Bitbucket repositories for automated testing.	Data is non-personalised or bound by other requirements