This policy applies to CX Services which trades as CX Services Ltd, and any other Company within the CX Services Ltd Group of Companies. Where reference is made to 'CX Services' or the 'Company' this refers to any of the Companies within the Group.

1. INTRODUCTION

1.1. This data retention, archiving and destruction policy (the "Policy") has been adopted by CX Services in order to set out the principles for retaining, reviewing and destroying data. This policy covers all employees (despite contract type) and all directors of CX Services, wherever they may be located or working.

1.2. This policy covers all the data retained or in the custody or control of CX Services, whatever medium data is contained in. This policy is not therefore restricted to information contained in paper documents but includes data contained in an electronically readable format. For the purposes of convenience, in this policy the medium which holds data is called: "a Document".

1.3. This policy should be read in conjunction with other policies that have as their objectives the protection and security of data such as the Privacy Policy and Security & Staff Confidentiality Policy.

1.4. OBJECTIVES

1.4.1. CX Services is bound by various obligations with regard to the data that we retain or that is in our custody or under our control. These obligations include how long we may retain data and when and how we can destroy it. The obligations may arise from local laws or regulations or from contracts and promises we have made to our employees, customer, goods and service providers and our partners.

1.4.2. Further, CX Services may be involved in unprecedented events such as litigation or business disaster recoveries that require us to have access to original Documents in order to protect CX Services interests or those of our employees, customers, goods and service providers and our partners.

1.4.3. As a result, Documents may need to be archived and stored for longer than the data may be needed for day to day operations and business processes. A contract may, for example, expire after two years but other Documents may, by law, need to be retained for a longer period.

1.4.4. Broadly, when the Documentation Retention Period is over and we no longer need the Document, we ought to destroy it in a proper manner.

2. RETENTION POLICY

2.1. Retention is defined as the maintenance of documents in a production or live environment which can be accessed by an authorised user during the ordinary course of business. For the avoidance, of doubt, Documents used in staging, development and testing or draft versions of Documents shall not be retained beyond their active use period nor copied into production or live environments.

2.2. The retention period of a Document shall be an active use period based by department and type as per Appendix 1 unless an exception has been obtained permitting a longer or shorter active use period by the business unit or department responsible for the creating, using, processing, disclosing, storing and destroying the document.

2.3. After active use has expired and according to appropriate exceptions Documents shall be archived in accordance with section 3 until the Documents are destroyed in accordance with section 4.

2.4. For the purposes of enforcing retention in accordance with this policy each department is responsible for the Documents it creates, uses, stores, processes and destroys. A sample list of document types across CX Services by department is attached in Appendix 1. This list shall be maintained by each department.

2.5. Each head of department shall be responsible for enforcing the retention, archiving and destruction of Documents and communicating these periods to the relevant employees.

2.6. Each head of department shall be responsible for submitting the exception requires to the process, including consulting and receiving legal advice if necessary to justify making an exception under section 5.

2.7. The legal department may issue a litigation hold request to the head of the department which requires that documents relating to a potential or actual litigation, arbitration or other claims, demands, disputes or regulatory action be retained in accordance with the instructions from the legal departments.

2.8. Each employee shall be responsible for returning Documents in their possession or control to CX Services upon separation or retirement. Final disposition of such Documents shall be determined by the immediate supervisor in accordance with this policy.

3. ARCHIVING POLICY

3.1. Archiving is defined as secured storage of Documents such that Documents are rendered inaccessible by authorised users in the ordinary course of business but which can be retrieved by an administrator designated by the head of department for the Documents in question.

3.1.1 Paper Records shall be archived in a secured storage onsite or secured storage offsite location, clearly labelled in archive boxes naming the head of department, department and date to be destroyed.

3.1.2 Electronic records shall be archived in accordance with the CX Services Security Standards for access controls and in a format which is appropriate to the secure the confidentiality, integrity and accessibility of the Documents.

3.2. The archiving period of a document shall be based on department in Appendix 1 unless an exception has been obtained permitting a longer or shorter active use period by the head of department responsible for creating, using, processing, disclosing storing and destroying the Document.

3.2.1 An archiving period of more than that displayed by department in Appendix 1 may be granted by the exception for Documents with a vital historical purpose such as corporate records, contracts, technical knowhow. The head of department will request an exception in accordance with section 5 to archive Documents. Such exception request shall specify the administrative, organisational and technical measures to be undertaken to ensure confidentiality, integrity and availability of such documents.

3.2.2 An archival period of less than that displayed by department in Appendix 1 may be granted by exception for documents with a limited business purpose such as emails or to comply with client or industry requirements (for example PCI).

3.3. After the archival period has expired, Documents shall be destroyed in accordance with section 4.

3.4. For the purposes of enforcing archiving in accordance with this policy each department is responsible for the Documents it creates, uses, stores, processes and destroys. A sample list of Document types across CX Services by department is attached as Appendix 1. This list shall be maintained by each head of department.

3.5. The legal department may issue a litigation hold request to the head of department which requires that documents relating to potential or actual litigation, arbitration or other claims, demands, disputes or regulatory action be archived in accordance with instructions from the legal department.

3.6. Each head of department shall be responsible for enforcing retention, archiving and destruction of Documents, and communicating these period to the relevant employees.

4 DESTRUCTION POLICY

4.1. Destruction is defined as physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially available means.

4.2. CX Services shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files. Paper documents shall be shredded using secure external service.

5 EXCEPTIONS TO THE RETENTION PERIOD

5.1. Exceptions may be requested under the following circumstances:

5.1.1 The head of department shall review and submit to the CX Services Information Security Management Team an exception request to archive data for a different period as prescribed in Appendix 1. The reasons may be a client requirement, business requirement, legal requirement or vital historical purpose.

5.1.2 The exception request form shall be reviewed and approved by the CX Services Information Security Management Team and routed to head of department to enforce as shown in Appendix 2.

5.2. Documents for which the legal department has issues a litigation hold order shall be archived, retained and destroyed as specified by the legal department.

6. RESPONSIBILITIES

6.1. Heads of departments shall be responsible for implementing this policy and ensuring that employees understand this policy and that they preform processes and procedures to execute this policy.

6.2. The compliance department shall be responsible for auditing compliance with this policy and providing an audit report with recommendations to be reviewed by relevant senior management, CX Services Information Security Management Team and directors.

7. ENFORCEMENT AND REPORTING BREACHES

7.1. Breaches of this policy may have serious legal and reputation repercussions and could cause material damage to CX Services. Consequently, breaches can potentially lead to disciplinary action that could include summary dismissal and to legal sanctions, including criminal penalties.

7.2. All employees are expected to promptly and fully report any breaches of the policy. A report may be made to the employee's supervisor or to the CX Services Information Security Management Team. Reports made in good faith by someone who has not breached this policy will not reflect badly on that person or their career at CX Services. Reports may be made using the following email address: compliance@cxservicesltd.com

Appendix 1: RETENTION PERIOD

Department	Data Type	Retention Period	Archival Period
HR/Accounts	Employee data Financial data	2 years	7 years
GTS	Mailing Data Test Data	6 months	6 months
	Data stored in Database	Indefinitely	Not Applicable
Operations	Mailing Data Captured Data Emailed Data Requests Text Requests Returns	6 months	6 months
	Coupons	3 months	Not Applicable
	Call Recordings	90 Days	Not Applicable
Client Services	Mailing Data Captured Data Emailed Data Requests Text Requests Returns	6 months	6 months
	Coupons	3 months	Not Applicable
	Client Emails Job Briefs Contractual Quotes	2 years	2 years
Sales and Marketing	Client Emails Job Briefs Contractual Quotes Tender Information	2 years	2 years

Exception Process	Rationale and Process
Request to destroy records in advance of schedule	Provide rationale to CX Services Information Security Management Team, ISM team to then send approval to destroy to GTS
Request to retain records and archive rather than destroy	Provide rationale to CX Services Information Security Management Team, ISM team to then send approval to GTS to archive

Appendix 2: EXCEPTION REQUEST / LITIGATION HOLD FORM

Information Security Exception Request Form

Instructions:
The Information Security Exception Request from below is required whenever a department within CX Services would like to deviate from the CX Services Data Retention, Archiving and Destruction Policy. The instructions below is designed for heads of departments when requesting an exception to the standard retention schedule of active use as outlined in Appendix 1 of the policy.

The type of exception you can submit is:
To obtain approval to archive data for less than the archival period in Appendix 1 and destroy it.
To obtain approval to archive data for more than the archival period in Appendix 1 and stop its destruction.
Submit this form to the CX Services Information Security Management Team for approval or rejection.

Item	Item Description	Explanation
1.	Policy Name	E.g. Data Retention, Archiving and Destruction Policy QA0158
2.	Reference	Your reference for request
3.	Location/Site	Insert your location site here
4.	Technology Scope: Name of Application/System/Database/Storage/Network Equipment	Insert the name of the application, system, storage medium or network equipment for which you propose the retention schedule
5.	Client Name	Insert client name if applicable to this request
6.	Client Contact Name	Insert client contact name if applicable to this request
7.	Client Contact Details	Insert client contact details here if applicable to this request
8.	Description and Reason for exception	
9.	Description of risk associated with exception	CX Services is committed to ensuring adequate information security which includes retaining, reviewing and destroying information when such information no longer serves a

		business purpose. Absent such controls, CX Services is at risk of contravening its obligations under our security policy and applicable data protection laws for which monetary fines, contractual penalties and reputational harm can result.
10.	Client consent request	If client is requesting exception please provide link to documentation from client asking for request
11.	Anticipated duration for exception	
12.	Ownership to accept risk	
13.	Additional information from requester (if required)	

Important note

This exception request form should be used only if there is a clear legal or business need to either retain or destroy the data in question.

Requester's Information (To be filled in by the requester)

Name:	**Designation:**	**Phone:**	**Email:**	**Location/Site**

1.	Policy Name	Data Retention, Archiving and Destruction Policy QA0158
2.	Reference	
3.	Location/Site	
4.	Technology Scope: Name of Application/System/Database/Storage/Network Equipment	
5.	Client Name	
6.	Client Contact Name	
7.	Client Contact Details	
8.	Description and Reason for exception	
9.	Description of risk associated with exception	
10.	Client consent request	
11.	Anticipated duration for exception	
12.	Ownership to accept risk	
13.	Additional information from requester (if required)	

CX Services ISMT Decision (Approval/Rejection) For ISMT Use Only

Decision on Exception Request	□ Approved	□ Rejected	□ More Info Needed

#1 Name: Signature: Date: