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

CX Services is a data controller and data processor and holds its own data (financial, supplier and employee) and client data. All data needs to be protected.

The object of this policy is to contain any breaches, to minimise the risk associated with the breach and to consider what action is necessary to secure personal data and prevent further breaches.

2. RESPONSIBILITY

This policy shall be understood and followed by all members of staff.

3. TYPES OF DATA BREACH

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include but are not limited to:

- unauthorised use of, access by or modification to data, buildings or IT systems
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- unauthorised disclosure of sensitive / confidential data
- loss of availability of personal data.

A data breach is an event or action which may compromise the confidentiality, integrity or availability of personal data or database systems, either accidentally or deliberately.

4. REPORTING AN INCIDENT

On discovering a breach or a suspected breach this should be reported through the Intranet on the 'DATA BREACH REPORT FORM'.

Section 1 of the report form will capture:

- Date incident was discovered
- Date of incident
- Place of incident
- Name of person reporting the incident
- Contact details of person reporting the incident
- Brief description of the incident or details of the information lost
- If client data – type of data such as letter or data list.
- If CX Services Data – type of data such as employee, supplier or financial
- Description of action taken at the time of the discovery.

5. CONTAINMENT AND RECOVERY

On receipt of the notification of a breach the DPO or appointed person will determine if the breach is still occurring, if so appropriate steps will be taken to minimise the breach.

An initial assessment will be taken by the DPO or appointed person in liaison with the relevant team members to establish the severity of the breach and who will take the lead in investigation the breach as the Investigation Officer (IO)

6. ASSESSMENT OF SEVERITY

The DPO or IO will undertake an in depth assessment in consultation with the IT Director. The investigation will be undertaken within 24 hours of the breach being reported. The IO will investigate the breach and assess the risks associated with it.

Section 2

- Type of data involved
- its sensitivity
- what's happened to the data – has it been lost or stolen
- could the data be put to illegal or inappropriate use
- who's data has been affected Client, CX Services, Supplier, Employee
- who the individuals are, number of individuals and potential effects on the data subjects.
- whether there are wider consequence's to the breach

The IO, DPO in consultation with the Managing Director and IT Director will determine who needs to be notified of the breach.

Every incident will be assessed on a case by case basis, however, the following will need to be considered:

- whether there are any legal / contractual notification requirements.
- whether notification would risk the individual affected
- whether notification would help prevent the unauthorised or unlawful used of personal data
- if a large number of people are affected or there are serious consequences and this is CX Services owned data then whether the ICO should be notified if personal data is involved (the client will notify the IOC if the data is client owned https://ico.org.uk/for-organisations/report-a-breach
- the dangers of over notifying. Not every incident warrants a notification.

Notifications to any individuals whose personal data has been affected by the incident will include:

- a description of how and when the breach occurred and the data involved.
- what action has been taken to mitigate the risks.

Consideration should be given to notifying third parties such as police, insurers, bank or credit card companies. This would be appropriate where there is a risk illegal activity may occur.

7. EVALUATION AND RESPONSE

Once the initial incident is contained and has been investigated the IO or DPO will carry out a full review, this will be documented in an NCR and signed off on Section 3.

This will include:

- a full review of causes of the breach.
- the effectiveness of the response.
- whether changes to systems, polices, flow charts, staff training or procedures should be made.
- existing controls will be reviewed to determine adequacy and whether corrective actions should be made.

If deemed necessary further corrective actions will be identified and implemented to ensure there is no repetition.