Storing and transferring data policy

Revision History				
Date	Version	Author	Summary of Change	Change made by
15.01.2016	1.0	Chris Scott	New version	N/A
17.03.2016	1.1	Chris Scott	New template	SCW
15.04.2018	1.2	Chris Scott	GDPR Update	AS

Approval			
Date	Version	Approver	Title
15.01.2016	1.0	Phil Miller	Managing director

Introduction

This Policy covers the storage and transferring of data. Employees at ABCA Systems are given a variety of resources to carry out their jobs efficiently and effectively. However, it is important that these resources are carefully guarded.

Storing, transferring and sharing company information comes with risks and can result in the following:

- *Data breaches*; company data is released to people outside of the organisation or employees of the organisation who haven't been granted access to it.
- *Data theft*; hackers steal information for financial gain or to gather intelligence.
- *Misplaced data*; original files become lost or unavailable.

Purpose

The purpose of this policy is to ensure that data is kept available only to current employees of ABCA Systems Ltd. who have been pre-approved to possess it.

The Benefits of a storing and transferring data Policy

The benefits of this policy are that there is clarity and guidance for any employee who may accidently misplace a storage device or send sensitive data incorrectly. The guide can also be used by employees for guidance in order to prevent anything being misplaced accidentally.

How to store and transfer data securely

Email

- All data sent over email (as an attachment or in an email text) should be considered sensitive and protected as such, so you should never send work documents or information to someone outside of the company unless it has been authorised by your line manager (this includes forwarding company emails to your own personal email account).
- Not all users within ABCA Systems have access to the same information so before sending data or files to a co-worker in an email, check with your line manager to ensure the recipient is allowed to have access to it.
- Documents should be protected by password, if it contains personal data

Cloud storage and cloud applications

- Workers may sometimes need remote access to work outside of the office from home, via mobile devices or company equipment on the road.
- Work information should never be stored or shared to personal cloud accounts or applications, such as iCloud, Google Drive, Box, Dropbox, Microsoft OneDrive, etc.

Physical storage devices

- Storing work data on physical devices is only permitted if pre-approved by your line manager

Social media for work data

- Work data or information must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.
- A complete social media policy (ASLPD2013) is in place.

Encryption

- While encrypting data may not prevent a data breach, it can help ensure that if information falls into the wrong hands it can't be read or used.
- If information is required to be encrypted, it must be protected by a strong password and the password sent separately to the data. Information should never be copied or shared in a way that would make it available outside of the encryption process.
- All laptops will be encrypted to protect data when this device is moved from an ABCA office.

Whenever you have any doubt or questions on data transfers, contact your line manager before doing anything else.