Mobile Computing and Remote Access Policy

Revision History				
Date	Version	Author	Summary of Change	Change made by
15.01.2016	1.0	Chris Scott	New document	NA
16.03.2016	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

Policy Statement

Staff working remotely must ensure that they work in a secure and authorised manner as set out in the Key principles below.

Who is covered by the Policy?

This remote access policy applies to all staff who use or access ABCA Systems Ltd. systems or information from a remote site, either occasionally or as part of their day to day employment. This policy covers information in all formats, including manual records and electronic data.

Remote working means working outside of a recognised ABCA office of from home, but it also includes working while connected to the an ABCA Wi-Fi network when office based.

Staff includes anyone working on behalf of the company

This policy sets out policy and guidance on how staff can work remotely in a secure and low risk fashion.

Scope of the Policy

This policy is to ensure that staff are aware of their individual responsibilities around information security when working remotely, and to provide guidance to all staff on secure remote working and so minimise any risk of unauthorised access to, and loss of, data.

Risks and Benefits of Remote Access

Staff may have remote access to information held on secure servers, but without the physical protections available on site and the network protections provided by firewalls and access controls, there are much greater risks of unauthorised access to, and loss or destruction of, data. There are also greater risks posed by information 'in transit'.

Types of risk:

- **Reputational risk**; the loss of trust or damage to ABCA Systems Ltd. relationship with its customers.
- **Personal risk**; the unauthorised loss of, or access to, data which could expose employees to identity theft, fraud or significant distress.
- **Monetary risk**; the ability for UK or overseas authorities to impose financial penalties.

Roles and Responsibilities

Any ABCA Systems Ltd. employee who works remotely is directly responsible for ensuring that they work securely and protect both information and ABCA-owned equipment from any loss, damage or unauthorised access.

Line managers are responsible for supporting their staff adherence with this policy. Failure to comply with this policy could result in disciplinary action.

Key Principles

All staff must comply with the following key principles when working remotely:

- Staff should be authorised to remotely access company information or systems by their line manager.
- Do not use IT equipment where it can be overlooked by unauthorised persons and do not leave it unattended in public places.
- Use automatic lock outs when IT equipment is left unattended.
- Ensure that the master copy of the record, whether paper or electronic, is not removed from ABCA premises. In identifying master copies of record, staff should seek advice from their line manager.
- Where possible, IT equipment must be encrypted.
- You should not work remotely if there is a risk to your health or safety, for example during building work at home or in unsanitary conditions, or if there is not a satisfactory work space for you to use. It is your responsibility to ensure that the working environment and space is suitable for remote working.
- Do not use non-authorised ways of working or remote working products, like GoToMyPC or using internet cafes, when accessing company systems and data. VPN is the only ABCA authorised way of working remotely and any exceptions must be authorised in advance by your line manager.
- Access to certain systems and services by those working remotely may be deliberately restricted or may require additional authentication methods. Any attempt to bypass these restrictions may lead to disciplinary action and could be classed as gross misconduct.
- When the company provides IT equipment to staff, it will supply devices which are appropriately configured to ensure that they are as effectively managed as devices in the secure office environment.

Staff who have been provided with company IT equipment to work remotely must:

- Only use this equipment for legitimate work purposes;
- Not modify it under any circumstances; and
- Not allow non-staff members (including family and friends) to use the equipment.

Users who work remotely on privately-owned equipment are responsible for the security of the device.

Staff working remotely must adhere to the company's Data Retention and Destruction policy (ASLPD201) and in particular ensure that information held remotely is securely deleted or destroyed once it is no longer necessary to be worked on remotely.

All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any ABCA-owned IT equipment or data immediately to their line manager, in order that appropriate steps may be taken quickly to protect company data. Failure to do so immediately may seriously compromise company security and, for staff, may lead to investigation and potentially action under the disciplinary procedures.

Please note that the company is not responsible for your remote working environment or desk and screen equipment.