Access control policy

Revision History				
Date	Version	Author	Summary of Change	Change made by
15/01/16	1.0	Chris Scott	New document	N/A
17/03/16	1.1	Chris Scott	Change of template	SCW

Approval			
15/01/16	1.0	Philip Miller	Managing Director

Introduction
Availability**,** confidentiality and integrity are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls.
Availability: – systems and information are physically secure and will be accessible to authorised persons when required.
Confidentiality - systems and information will only be accessible to authorised persons.
Integrity – the accuracy and completeness of systems and information are safeguarded.

It is vital for the protection of systems and information, that authorised users who have access to ABCA's systems and information are aware of and understand how their actions may affect security.

Authorised users referred to in this document are all parties (either as part of a contract of employment or third party contract) who have access to, or use of systems and information belonging to, or under the control of ABCA Systems:

Purpose
The purpose of this policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

Scope
The scope of this policy includes all access to information, systems and physical access to areas and locations where information and data of ABCA Systems is located. This policy applies throughout the information lifecycle from acquisition/creation, through to utilisation, storage and disposal.

Policy Statement
On-going education featuring induction programmes, line manager training and awareness programmes should be undertaken by staff to enable them to be aware of their responsibilities towards systems and information security.

SYSTEMS AND INFORMATION ACCESS.
Information owners, must explicitly define, document and keep up to date the access requirements for the specific roles which have access to the information.

Line Managers should notify HR if an employee's role within the company changes and access to systems and information needs to updated or removed. Managers must follow up and confirm that access to other systems and programs have been updated correctly.

- The appropriate level of access to systems and information will be determined upon the prospective users required business need, job function and role, and will be set at the induction stage. Any requests to amend access rights to any system should be made through the employees' line manager.
- A signed confirmation by the user may be required indicating that they understand and appreciate the conditions of certain access and security.
- If authorisation to use certain systems and information is granted, using a generic log in, then that log in must not be divulged to any other party.
- Access for remote users shall be subject to authorisation by line managers via the Mobile Computing & Remote Access Policy. No unauthorised external access to any network device or networked system shall be permitted.
- The application and all other documentation should be maintained in line with the all other company guidance.

SYSTEMS/INFORMATION DE-REGISTRATION

If a member of staff changes role or their contract is terminated, the line manager should ensure that a user's access to the system/information has been terminated. A follow up exit interview should also cover confirm the termination of system and information access rights.

- If an employee is deemed to have contravened any of this Access Control Policy or has unauthorised access to any systems or information, then their line manager should review their access rights to the system and information and report accordingly. The line manager should remind the user of this Policy and the relevant access and security aspects relative to the employee.
- If a number of unsuccessful log-on attempts are exceeded, the user will be informed that they need to contact their line manager and / or IT, to ask for access rights to be reinstated.
- The line manager should remind the user of this Policy and the relevant access and security aspects relative to the employee.
- If it is deemed that it is no longer appropriate or necessary for a user to have access to systems and / or information then the user's line manager will need to inform HR and or IT that access rights should be amended/removed immediately.
- If any system and / or information rights are amended or removed, the relevant system / information access records will need to be updated accordingly.

LOG-ON CONSIDERATIONS

- All systems should be accessed by secure authentication of user validation. As a minimum this should entail use of a User name and a Password.
- Logon to systems/information should only be attempted using authorised and correctly configured equipment
- After successful logon users should ensure that equipment is not left unattended and active sessions are terminated or the screen is locked as necessary. Systems should be logged off, closed down or terminated as soon as possible.
- System logon data should not be copied, shared or written down.

PHYSICAL ACCESS AND CONTROLS

Maintaining the physical security of offices where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data:

- Visitor ID badges should be issued to and worn by non-employees whilst on ABCA premises. Visitors who are not displaying ID badges should be challenged. Any person not known to employees must be challenged in order to establish who they are and whether authorisation has been provided for them to be on site. If there is any doubt about the identity of the individual, the appropriate line manager and / or HR should be contacted to confirm the individual's identity. DO WE HAVE A VISITOR ID PROCESS
- Appropriate recording mechanisms need to be in place in every ABCA premises to record the names, dates, times and signatures for the signing in and out of visitors. All visitors must be issued with a visitors badge when signing in.
- The use of keys and access control fobs to buildings, rooms and cabinets, must be controlled and recorded. Keys must be stored in secure areas and the location of keys must be known at all times.
- Electronic access control fobs must be issued to authorised staff on an individual basis and programmed according to the employees' role and requirement to access physical areas storing systems and / or information. Staff issued with access fobs must have their names recorded against the registered access fob number including date and time of issue, and access rights.
- Access control fobs should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. There should not be any tailgating whilst entering ABCA premises or protected areas within office of ABCA Systems.
- In emergency situations, authorised personnel may be permitted to use another authorised person's fob if available with permission of the line manager and the recorded user must either be present or be made aware that their fob is being used. Any such use must be recorded and maintained in a logging system for this type of event

- If electronic door locks and / or access control fobs are in use they must be issued to authorised staff on an individual basis, be fully registered to that individual and only used by that individual.
- Access control fobs issued to personnel who no longer work for the company must be deactivated and recovered immediately. A follow up exit interview should also cover confirm the return and deactivation of access control fobs.
- Locations housing critical or sensitive information and/or information processing facilities should have secure access controls and restrictions allowing access to authorised staff only.
- Observance and maintenance of the physical security of rooms where PCs and / or critical information processing equipment is located needs to be a paramount consideration, as should the provision of adequate environmental and fire controls in those rooms
- Access to information processing systems will only be allocated to staff following any required checks. If required, usage policies will also need to be signed by staff.
- All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.
- Access to and knowledge of key fobs, door lock codes or access to keys for locks, are restricted to authorised personnel only and must not be shared with any unauthorised person.
- Access codes used for any secure locking mechanisms or alarms must be changed every six months as a minimum or more regularly in line with professional best practice. Outside of ABCA Systems head office, a record should be kept in a secure location of when the dates when the access codes are updated.
- Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms with access control.
- All Third Party Contractors must have and display appropriate identification and be made aware of the requirements within this procedure.
- Personal, special access visits from relatives or acquaintances of personnel are not permitted within secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure.

Responsibilities

Directors are responsible for ensuring that all staff and line managers are aware of security policies and that they are observed. Line managers need to be aware that they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems, and have been made aware of their responsibilities towards security.

Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to company assets, or an event which is in breach of the company's security procedures and policies.

All ABCA employees have a responsibility to report security incidents and breaches of this policy as quickly as possible through their line manager or direct to HR. This obligation also extends to any external organisation contracted to support or access the company's information and systems.

ABCA Systems will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines. In the case of an employee then the matter may be dealt with under the disciplinary procedures.