Information Security Policy Statement

1. Purpose

This policy provides a framework for the management of information security throughout the company. It applies to:

1. All people with access to the company information systems, including employees, visitors and third/external parties (including contractors).
2. Any systems attached to or supplied by the company. This includes computer and telephony devices.
3. Any data that the company processes, regardless of whether it is in hard or electronic copy and any communications sent to/from the company. This also includes any company data residing on non-Company external systems.
4. All third parties that provide services to the company that may have access to the data.

2. Aims

The company recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the company's activities and are essential.

The company have a Quality Manager (QM) who is responsible for information security throughout the business. This person, along with the company directors, are responsible for authorising, advising and ensuring the information security directives are applied throughout the organisation. An external IT support/consultancy contractor is used to carry out the technical work required as well as to advise on security.

Confidentiality, integrity and availability of information is integral to the company and could prevent the company from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information has the potential to damage the company's reputation and cause significant financial loss.

To mitigate these risks, information security must be an integral part of information management.

The Company protects the security of its information systems in order to ensure that:

1. Information is accurate and updated.
2. Information is available to those who require it when they require it.
3. Information is restricted to those who require it. Access to information is restricted via an authorisation process.
4. Legal requirements are met.
5. Reputation of the Company is safeguarded.

Reasonable information security risk assessments will be performed for all information systems on at least an annual basis. Any new systems or relevant work will be reviewed, the risk assessment undertaken and appropriate protection implemented.

The Company is committed to implementing education, policies, processes and procedures to assist users to ensure they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information.

The Quality Manager (QM) and the Directors of the Company, shall advise on best practice and coordinate the implementation of information security controls.

The Company will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

Breaches of information security must be recorded and reported to appropriate bodies in the Company, who will take action and inform the relevant authorities.

This Policy and all other supporting policy documents shall be communicated as necessary throughout the Company to meet its objectives and requirements.

3. Responsibilities

Quality Manager (QM)

This assigned person has ultimate responsibility for information security within the Company. This includes ensuring any legislation, ISO accreditations and other requirements are complied with. Where necessary the Directors of the business will be responsible for supporting the QM in order for the information security policy to be created, authorised, communicated, complied with and monitored.

QM and Directors

Due to the structure of the business it is not possible for the QM to address all aspects of the information security policy. Therefore, the QM works with Directors to:

1. Ensure that users are aware of this policy.
2. Provide adequate resources for its implementation.
3. Ensure compliance is monitored.
4. Conduct annual reviews of the policy. This must take into account relevant changes in legislation, organisational policies and contractual obligations.
5. Ensuring there is clear direction and visible management support for security initiatives.

Communication

Given the Company's devolved structure, the information security policies and other policies are published for users to access. There is a general company standard Communication Process which is used for security policy and other types of communications.

Users

Users of Company information will be made aware of their own individual responsibilities for complying with Company policies on information security. Where appropriate, training is provided. Any non-compliance of these policies may be subject to disciplinary.

Third/External Parties

Agreements with third parties involving accessing, processing, communicating or managing the Company's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

It will be communicated that all information provided or available should be treated as confidential at all times except for information held in the public domain or given express permission to be disclosed and to what extent.

4. Risk Assessment and the Classification of Information

4.1. Risk assessment of information held

The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

Given the devolved nature of the Company's structure, the risk assessment should be carried out in the first instance by the QM and if necessary, Directors.

The risk assessment should identify the Company's information assets; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to the department or Company as a whole. In assessing risk, departments should consider the value of the asset, the threats to that asset and its vulnerability.

Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

Rules for the acceptable use of information assets should be identified, documented and implemented. This is primarily located in the Employee Handbook which is a working document and made available to all users.

Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the Company's infrastructure, systems and processes.

The company's external IT Support/Consultancy partner will also bring to the Company's attention any risks that they identify.

4.2. Personal Data

Personal data must be handled in accordance with the Data Protection Act 1998 (DPA) and in accordance with the Company's policy and guidance on personal data.

The DPA requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

A higher level of security is provided for 'sensitive personal data', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

5. Company Information

All information is to be generally treated as confidential information. However, this can be a matter for assessment in each individual case. In a general sense however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

1. Financial loss.
2. Reputational damage.
3. An adverse effect on the safety or well-being of members of the Company or those associated with it.

5.1. Storage

5.1.1. Company information should be kept secure, using, where practicable, dedicated storage (e.g. file servers) rather than local hard disks, and an appropriate level of physical security. Information on local hard disks will not be backed up.

5.1.2. File or disk encryption should be considered as an additional layer of defence, where physical security is considered insufficient.

5.2. Access

5.2.1. Company information must be stored in such a way as to ensure that only authorised persons can access it. Confidential information will be even further restricted.

5.2.2. All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords. Password policies will be applied in order to force password good practices.

5.2.3. Where necessary, additional forms of authentication should be considered.

5.2.5. Users with access to confidential information should be vetted as appropriately by the QM and/or Directors.

5.3. Remote access

5.3.1. Where remote access is required, this must be controlled via the defined VPN or Remote Desktop Gateway. Access controls are in place via the Domain to allow the minimum access necessary.

5.3.2. Any remote access is controlled by secure access control protocols using appropriate levels of encryption and authentication.

5.4. Copying

5.4.2. The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where necessary, a record kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed (see 5.12.5).

5.4.3. All copies should be physically secured e.g. stored in a locked cupboard drawer or filing cabinet.

5.5. Disposal

Policies and procedures must be in place for the secure disposal/destruction of confidential information. The Company's policy on the disposal of old computers is referenced in section 7 of this document.

5.6. Use of portable devices or media

5.6.1. All portable devices should be kept secure at all times.

5.6.2. Data copied onto portable devices should be copied regularly onto central file servers otherwise there is a significant risk of data loss should an issue with the device occur.

5.6.3. The permission of the information owner should be sought before confidential information is taken off site. The owner must be satisfied that the removal is necessary and that appropriate safeguards are in place e.g. encryption.

5.6.4. No personal or explicitly-specified confidential data should be copied onto portable devices or media unless they are encrypted.

5.6.5. The passphrase of an encrypted device must not be stored with the device.

5.7. Exchange of Information and use of Email

5.7.2. Email is suitably protected using Office365 credentials.

5.7.3. Email should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken e.g. potentially some kind of encryption.

5.8. Cryptographic controls

5.8.1. Where deemed necessary, procedures should be in place to support the use of cryptographic techniques and to ensure that only authorised personnel may gain access to confidential information.

5.8.2. Company guidance on cryptographic policy and key management, can be obtained from the Company IT support/consultancy partner. If necessary it should be followed to ensure that data is appropriately secured and that all legal and regulatory requirements have been considered.

5.9. System planning and acceptance

A risk assessment should be carried out as part of the business case for any new ICT system that may be used to store Company and/or confidential information. The risk assessment should be repeated periodically on any existing systems.

5.10. Backup

Information owners should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all-important information assets should be taken and tested regularly in accordance with such an appropriate backup policy. In order to ensure this, all files and emails should be located on the company server infrastructure.

5.12. Hard Copies

Protective marking

5.12.1. Documents containing confidential information should be marked as 'Confidential' or with another appropriate designation e.g. 'sensitive', etc, depending on the classification system adopted by the department.

Storage

5.12.2.

a. Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers or cabinets. Where this is not practicable, and the information is kept on open shelving, the room should be locked when unoccupied for any significant length of time.

b. Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

Removal

5.12.3. Confidential information should not be removed from the Company unless it can be returned on the same day or stored securely overnight, as described in section 5.12.2 above.

Transmission

5.12.4.

a. If confidential documents are sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

b. If confidential documents are sent by external post, they should be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.

c. If confidential documents are sent by internal post the documents should be placed in an envelope marked 'Confidential' with the addressee's name clearly written on it.

Disposal

5.12.5. Confidential documents must be shredded in a confidential manner prior to disposal.

5.13. Enforcement

5.13.1. All users must be emailed periodically to update and remind them of the location of the Information Security Policy and their obligations. This will be via the Company Communication Procedure.

5.13.2. Any failure to comply with the policy may result in disciplinary action.

5.13.3. Any loss or unauthorised disclosure must be promptly reported to the owner of the information.

5.13.4. Computer security incidents involving the loss or unauthorised disclosure of confidential information held in electronic form must be reported to the QM or a Director as soon as possible.

5.13.5. If the loss or unauthorised disclosure involves personal data, whether electronic or hard copy, the QM or a Director need to be informed as soon as possible.

6. Compliance

6.1. The Company has established this policy to promote information security and compliance with relevant legislation, including the DPA. The Company regards any breach of information security requirements as a serious matter, which may result in disciplinary action.

6.2. Compliance with this policy should form part of any contract with a third party that may involve access to network or computer systems or data.

6.3. Relevant legislation includes, but is not limited to:

- The Computer Misuse Act 1990
- The Data Protection Act 1998
- Provision and Use of Work Equipment Regulations (PUWER 1998)
- Health and Safety Display Screen Regulations 1992
- Waste Electrical & Electronic Equipment Regulations 2006

7. Other Relevant Company Policies or Guidance

- CEH002 Employee Handbook
- CEH001 Employee Safety Handbook
- CCP004 Disposal of Waste Electrical & Electronic Equipment (WEEE) Guidelines
- CDT018 Display Screen Equipment Self-Assessment questionnaire
- CPS001 Quality Policy
- CPS003 Environmental Management System

Also, Data Protection: Other than for keeping staff records or for accounts purposes the Company does not process personal data. However, the following measures are followed: http://ico.org.uk/for_organisations/data_protection/security_measures

8. Contacts for Further Information

Name	Role	E-mail	Telephone Numbers
Lucy Harper	Quality Manager (QM)	lucy.harper@a1-es.com	0117 244 1856 07889 649898
Dean Frost	Managing Director	dean.frost@a1-es.com dean.frost@clade-es.com	0117 244 1856 07909 090466
Mike Atkinson	CEO	michael.atkinson@clade-es.com	0113 887 9604 07970 548696
Michael Hodgson	Finance Director & IT Management	michael.hodgson@a1-es.com	0117 244 1866 07793 600248