Information Handling Policy

1. Introduction

This Information Handling Policy is a sub-policy of the Information Security Policy and sets out the requirements relating to the handling of the Company's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation, which would otherwise occur.

2. Security classification

Each information asset category will be assigned a security classification by the asset owner, which reflects the sensitivity of the asset according to the following classification scheme:

- Public – available to any member of the public without restriction.
- Open – available to any authenticated member of the Company.
- Confidential – available only to specified members, with appropriate authorisation.
- Strictly Confidential – available to only a very small number of members, with appropriate authorisation.
- Secret – the most restricted category. It is not anticipated that many Company assets will be assigned this classification.

Any information which is disclosable under the Freedom of Information Act 2000 will be classified as public. Any data which is classified as sensitive personal data under the Data Protection Act 2018 (or its successor legislation) will be classified as strictly confidential.

4. Access to information

Members of the Company will be granted access to the information they need in order to fulfil their roles within the Company. Staff who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

5. Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely. Confidential paper waste must be disposed of in accordance with formal Company procedures and will be shredded in the first instance.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Company, unless the disposal is undertaken under contract by an approved contractor, as detailed in the IT disposal policy.

6. Removal of information

Company data, which is subject to the Data Protection Act or which has a classification of confidential or above should be stored using Company facilities or with third parties subject to a formal, written legal contract with the Company, wherever possible. In cases where it is necessary to otherwise remove data from the Company, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Strictly confidential data in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner. (See the Cryptography policy). Particular care needs to be taken when information assets are in transit.

7. Using personally owned devices

Data subject to the Data Protection Act must never be stored on personally owned devices. Data classified as sensitive under the Data Protection Act must neither be stored on nor processed using personally owned devices.

Personally owned devices should not be used for the storage or processing of any other information classified as strictly confidential or above without the explicit written permission of the data owner. Appropriate security measures must be taken when using personally owned devices to process or store any Company data.

8. Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. Staff offices should be locked when empty.

9. Backups

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

10. Exchanges of information

Whenever personal data or other confidential information is transmitted to or exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred.

Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as strictly confidential may only be exchanged electronically both within the Company and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified, as secret may not be transmitted electronically except with the explicit written permission of the information owner.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Staff or contractors of the Company must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

11 Reporting losses

Any member of staff or contractor working behalf of the Company has a duty to report the loss, suspected loss or unauthorised disclosure of any Company information asset to the MD.

Signed by Dr Adnan Niazi

Dated 4/1/2021
Last Reviewed On 05/07/24

Version 1