Information security policy

Author: Information Security Manager

Classification: Public

Revision History

Date	Version	Revised by	Notes
04/05/2018	1	Information Security Manager	Split from Group IT communication and security policy
10/08/2018	1.1	Information Security Manager	Classification change to 'Public'
12/06/2019	1.2	Information Security Manager	Changes to: Section 2, 8 and 9.
26/08/2020	1.3	Information Security Manager	Addition in Section 7.1 to 'Restricted'

Document Distribution

This policy is available in accordance with internal classification procedures and is available on request.

Information security policy

1. Introduction

1.1. The company commits to keeping information secure; maintaining confidentiality, integrity and availability where appropriate and legal. Ensuring the protection of all information systems (including but not limited to all computer systems, mobile devices and data in all media).

1.2. Failure to adequately secure information can damage the business and the Company's reputation. Breach of this policy will be dealt with under Disciplinary Procedures and in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.3. This policy may be amended at any time to ensure that the company is adhering to current international standards for information security management system (ISMS).

2. Objectives

2.1. To provide a framework for establishing suitable levels of information security for all Adler & Allan systems to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

- 2.1.1. Ensure ISO27001:2013 standards are maintained within the Group
- 2.1.2. Retain Cyber Essentials and maintain PCI DSS standards
- 2.1.3. Comply with all Legislation and regulations related to information security (including the General Data Protection Regulation)

2.2. Information security awareness training is to be delivered to all staff at least once per calendar year (see section 2.1.3).

2.3. Receive positive recommendations with all continuing assessments (see section 2.1.1)

3. Scope

3.1. This policy is applicable to, and will be communicated to all staff, contractors, or any person(s) associated with Adler & Allan that interact with information held by Adler & Allan and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to the Adler & Allan data network, systems managed by Adler & Allan, mobile devices used to connect to Adler & Allan, networks which hold Adler & Allan data, data over which Adler & Allan holds the intellectual property rights, data over which Adler & Allan is the data owner or data custodian and communications sent to or from the Adler & Allan.

4. Definitions

4.1. **Data –** Information stored on computer systems or paper.

4.2. **Sensitive information –** Confidential and/or personal information that if lost or stolen could be detrimental to the company and/or individuals.

4.3. **DPIA –** Data Protection Impact Assessments

4.4. **GDPR –** General Data Protection Regulation

4.5. **IS –** Information Security

5. Legal Obligations

5.1. The company fully adheres to the current laws and regulations enforced within the United Kingdom (see appendices for a non-exhaustive list) as well as a variety of regulatory and contractual requirements.

6. Information security principles

6.1. Privacy by Design

The company incorporates the privacy by design approach, using DPIA's where necessary in new projects or projects where there is a change in the process of personal information.

The privacy by design approach is designed to help minimise privacy risks and build trust. The approach will help identify problems early and give the company ample time to meet our legal obligations and be less likely to breach the GDPR.

Projects that will require a DPIA:

6.1.1. New IT systems for storing and accessing personal data

6.1.2. Data sharing initiatives where two or more organisations seek to pool or link sets of personal data

6.1.3. Profiling of any kind

6.1.4. Using existing data in a new or more intrusive purpose

6.1.5. Surveillance systems (e.g. CCTV)

6.1.6. New databases which consolidate information held by separate parts of an organisation

6.1.7. Legislation, policy or corporate strategies which impact on privacy through the collection of information.

6.2. Staff with responsibilities (see section 9) for information must ensure the proper classification of that information (see section 7.1).

6.3. Information will be both secure and available with a legitimate need for access. Information access will be based on 'least privilege' and 'need to know'.

6.4. Information will be protected against unauthorised access and processing in accordance with its classification level.

6.5. Breaches of policy must be reported (see section 10).

6.6. Information security will be reviewed yearly through the use of internal audits, penetration testing and training.

7. Data Classification

7.1. All data is classified using the table below.

Classification (Level)	Definition	Examples
Confidential (High)	Information of great importance to either a person or the business that if breached could be detrimental to the aforementioned.	Sensitive personal data as defined by the GDPR (See appendices) Salary information Usernames and passwords Customer bank and payment details Customer contracts Company Data and data back ups Company accounts
Restricted (Medium)	Information designated for specific members of staff.	Personal data as defined by the GDPR (See appendices) CCTV systems Information system management procedures. Company Data Information Systems Adler & Allan Ltd Customer Portal

Internal (Low)	Information for all employees of the company.	Internal correspondence Intranet Policies and procedures
Public	Company information that is accessible to anyone	Company legal information Public policies (e.g. Privacy policies) Company website

7.2. Confidential information has been classified as highly sensitive information and the utmost care must be taken when storing and processing. Special measures must be taken with confidential information and authorisation must be granted at senior management level before any processing or transfers take place.

7.3. Restricted information has been classified as sensitive information and must be stored and processed securely. Role-based access must be reviewed as part of the ISMS Access control review.

7.4. Internal information must not be disclosed to the public. Internal information may be reclassified as public if contents have been redacted and authorised by senior management or Director.

8. **Clear desk & clear screen policy**

This policy is designed to prevent unauthorised access to sensitive information. The company requires all staff to maintain a clear screen and desk environment.

8.1. Employees should logically lock their PC when not at their desk.

8.2. Employees must protect confidential and restricted information (e.g. using lockable cupboards, filling cabinets and the like).

8.3. Employees should leave their desk clear at the end of their working day.

9. Responsibilities

9.1. Management responsible for information security (champions)

Executive Team
Head of Marketing
Information Security Manager
Group IT Manager
Human Resources Manager
Head of Health & Safety
Head of Procurement
Credit Manager
Group Finance Controller
Management Systems Coordinator
Quality Manager
Contracts Manager
Health & Safety Managers
Group Marketing Managers

9.2. All users are responsible for Information Security within their roles and responsibilities

10. Incident Response

10.1. All employees are required to keep vigilant regarding the handling or processing of information.

10.2. Employees should use the list below as an example of what may be classed as an incident.

10.2.1. Violation of company security policies

10.2.2. Unauthorised computer access

10.2.3. Loss of data confidentiality or availability

10.2.4. Compromised data integrity

10.2.5. Denial of service condition against data, network or computer

10.2.6. Misuse of company systems and/or equipment

10.2.7. Physical damage to company systems and/or equipment

10.3. If an employee is aware of an information security incident they must inform the company immediately using formal internal procedures.

11. Subject Access Requests (SAR)

11.1. All SAR's must be sent to informationsecurity@adlerandallan.co.uk.

11.2. SAR's must be processed within one month of the request being received in accordance with data protection laws.

12. Cryptography

12.1. All mobile devices (Mobile Phones, Tablets and Laptops) should be protected using the company encrypted mobile device management system.

12.2. Site-to-site traffic must be encrypted

12.3. Websites used by and operated by the company must use strict HTTPS throughout the whole site.

12.4. Remote workers (teleworkers) must connect to the company network externally using the authorised secure VPN.

13. External or Cloud Providers

13.1. All external providers must complete a security questionnaire as part of the supplier and sub-contractor risk assessment process before being an acceptable provider of services for the Adler & Allan Group.

13.2. Providers must operate in a secure manner, enforcing a secure development policy where necessary.

14. Disciplinary

14.1. Breach of this policy will result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate fully with any investigation.

15. Supporting Policies

15.1. This policy is supported by various policies within the Information security management system.

16. Contact Us

Email: informationsecurity@adlerandallan.co.uk

Address: Information Security, 80 Station Parade, Harrogate, North Yorkshire, HG1 1HQ

Appendix

1. Classification expansion information

Personal data

- The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

- The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

- Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

- "Special categories" - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

2. Legislation

2.1. The General Data Protection Regulation (or Data Protection Act 2018)

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The Computer Misuse Act 1990

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

2.2. The Freedom of Information Act

The Freedom of Information Act 2000 provides public access to information held by public authorities.

It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.