Classification: Public

Contents

1 Purpose

1.1 Information is a valuable asset that must be protected from unauthorized access, theft, misuse, loss, and corruption. Effective protection ensures business continuity, minimizes risk of financial loss, maintains legal compliance, and protects Adler and Allan's reputation. Poor training or breach of security controls can expose information to such risks. This policy defines a structured approach to mitigating risks related to information handling by implementing appropriate information security controls, as per ISO 27001:2022. This policy aligns with the 'Information Risk Management Procedure' and 'Data Protection Policy' to ensure holistic risk-based security management.

2 Objectives

2.1 Adler and Allan's key security objectives are to:

- **a** Retain certifications for ISO/IEC 27001:2022, Cyber Essentials, and PCI DSS.
- **b** Achieve 70% completion for information security awareness across staff.
- **c** Ensure compliance with all relevant legislation and regulations related to information security.
- **d** Enhance physical security across the group through improved CCTV, Access Control systems, and Visitor Management procedures.
- **e** Identify and mitigate risks arising from third-party engagement.

3 Scope

3.1 The Information Security Policy applies to all information assets at Adler and Allan, regardless of format, and extends to external organizations processing information on behalf of Adler and Allan. This policy covers all individuals with access to the company's information and technology, including third-party service providers.

4 Compliance Monitoring

4.1 The Information Security Team will monitor compliance with this policy. Results will be reported to the IT Director.

5 Review

5.1 This policy will be reviewed annually or as required by the Information Security Manager and approved by the IT Director.

6 Policy Statement

6.1 Adler and Allan is committed to safeguarding information assets from a loss of:

- **a** **Confidentiality**: Ensuring information is accessible only to authorized individuals.
- **b** **Integrity**: Maintaining the accuracy and completeness of information.
- **c** **Availability**: Ensuring information is available to authorized users when required.

6.2 The company will operate an Information Security Management System (ISMS) that meets certified standards and follows a risk-based approach for the application of necessary controls.

7 Information Security Policies

7.1 Adler and Allan will define lower-level controls, processes, and procedures to support the objectives stated in this high-level policy. The supporting documentation will be approved by the IT Director and communicated to relevant stakeholders.

8 Organisation of Information Security

8.1 Governance arrangements for information security will be established, with responsibilities clearly allocated to manage the security posture of the organization.

8.2 **Responsibilities:**

a **Board of Directors**: Accountable for the overall operation and compliance with information security policies.

b **Information Security Manager**: Responsible for implementing IS controls and policies, vulnerability testing, internal audits, IS training and awareness, and acting as the Data Protection Officer (DPO). The manager will maintain the IS risk register and oversee investigations related to cyber incidents, notifying regulatory bodies, insurers, and clients as needed.

c **IT Operations Manager** (formerly 'Group IT Manager'): Ensures the availability of information systems, manages change and patch processes, oversees disaster recovery tests, and is responsible for IT infrastructure investigations.

d **Compliance Team**: Ensures compliance with the ISMS framework and performs audits against information security controls.

e **Human Resources Manager**: Responsible for employee information security across the employment lifecycle.

f **Contracts Manager**: Ensures confidentiality is maintained throughout contract lifecycles.

g **Procurement Manager**: Ensures supplier onboarding processes comply with all relevant legislation.

h **Managers**: Ensure fair application of IS policies and procedures, and compliance by their teams.

i **Users**: Responsible for protecting information and devices, reporting suspicious activity, and complying with IS policies.

9 Human Resources Security

9.1 All users will be made aware of security policies and acceptable use standards. Information security education will be provided, and security responsibilities will be incorporated into role descriptions and development plans.

10 Asset Management

10.1 Assets, including information, software, hardware, and personnel, will be documented, classified, and assigned owners responsible for their maintenance. Each asset will have a defined retention and disposal schedule based on its classification.

11 Access Control

11.1 Access to information will be controlled based on business needs. Access levels will be assigned according to user roles and information sensitivity. Formal user registration and de-registration procedures will ensure proper authentication, and additional controls will be in place for users with elevated privileges.

12 Cryptography

12.1 Adler and Allan will use cryptographic methods to protect information confidentiality, integrity, and authenticity, providing appropriate tools and guidance for their use.

13 Physical and Environmental Security

13.1 Information processing facilities will be housed in secure areas protected by layered security controls to prevent unauthorized access, damage, or interference.

14 Operations Security

14.1 The correct and secure operation of information systems will be maintained through:

14.2 Documented operational procedures.

14.3 Formal change and capacity management.

14.4 Malware protection.

14.5 Defined logging practices.

14.6 Vulnerability management.

15 Communications Security

15.1 Network security controls will be implemented to protect information within Adler and Allan's networks. Secure transfer methods will be provided for sharing information both internally and externally.

16 System Acquisition, Development, and Maintenance

16.1 Information security requirements will be incorporated into system development and maintenance processes. Controls will be applied to mitigate risks, and test environments will be separated from operational systems.

17 Supplier Relationships

17.1 Supplier agreements will reflect Adler and Allan's information security requirements, and supplier activities will be monitored according to the sensitivity of the information involved.

18 Information Security Incident Management

18.1 Guidance will be provided on identifying and reporting security incidents. All incidents will be investigated, and corrective actions will be taken.

19 Business Continuity Management

19.1 Business continuity plans will protect critical processes from major system failures or disasters. Regular testing and impact analysis will be performed.

20 Compliance

20.1 All information systems must comply with statutory, regulatory, and contractual security requirements, including:

a Data protection legislation.

b PCI-DSS standards.

c Adler and Allan's contractual commitments.

20.2 Internal and external audits will verify compliance, and IT health checks will be conducted regularly.

21 Disciplinary

21.1 Any breach of this policy will result in disciplinary action, up to and including dismissal, depending on the severity of the breach. All employees are expected to cooperate with investigations fully.

22 Appendix 3. Incident Guide table

Action		**Damage*/loss/stolen uncategorised equipment** All PC and mobile devices	**Damage/loss/stolen categorised equipment**	**Witness breach of policy** Password secrecy, unattended equipment, unauthorised access to information.	**Malicious code or attempt at delivering** Where malicious code, malware or virus is suspected or known. Phishing included.	**Suspect/Unknown device** Unknown equipment found	**Unauthorised physical access** Known access to restricted area or intruders	**Data breach involving PII**	**Data or financial Loss** Results of social engineering or fraud.
Immediate	Report to IT Support/Security	☐	☐	☐	☐	☐	☐	☐	☐
	Report to SHEQ team	X	X	X	X	X	☐	X	X
	Stop using equipment	☐ *	☐	X	☐	☐	X	X	X
	Investigation team to notify the executive team	X	X	X	X	X	☐	☐	☐
Company action within 24 hours	Return equipment to line manager/System administrator	☐ *	X	X	X	X	X	X	X
	Report initial findings	☐	☐	☐	☐	☐	☐	☐	☐
Further action needed	Security manager or IT manager to investigate	☐	☐	☐	☐	☐	☐	☐	☐
	Security manager or IT manager to notify contract owner with details	☐	☐	☐	☐	X	X	☐	X
	DPO to notify authorities with details within 72 hours if required	X	X	X	X	X	X	☐	X

	Notify interested parties (insurers, third parties etc…)	X	☐	☐	☐	X	X	☐	☐
	Report results to the board	X	☐	X	☐	☐	☐	☐	☐

Contact Information

Email	**itsupport@adlerandallan.co.uk (IT and data Incidents)** **SHEQ@adlerandallan.co.uk (Depot/personnel Incidents)**		
	Information security Manager	**01423 850 360**	**07821 644067**
Telephone	**ARC Systems Helpdesk**	**01268 288 100 (Option 1)**	
	Mike Jordan ***IT Operations Manager***	**01993 222 999**	**07917541595**
	Lynda Wright ***Group Quality Manager***		**07836566526**

23 Revision History

Date	Version	Revised by	Notes
07/10/2024	Version 1.9	Stanley M	Reviewed, Updated
15/11/2024	Version 1.9	Neil R	Signed Off