Information Security Management Policy

Policy No: SPOL001

AdEPT

Document information

Versions and releases

Version	Date Released	Change Notice	Pages Affected	Description of revision
1.0	12/12/2017			Initial
1.1	04/07/2019			Removed AdEPT Telecom reference to AdEPT Technology Group
1.2	26/07/2022			Rebrand

Review History

Version	Date Released	Change Notice	Pages Affected	Description of revision
1.0	04/07/2019	Gary Noble	All	Company name change
1.0	05/07/2019	Gary Noble		No change Required
1.2	26/07/2022	Gary Noble	All	Rebrand

Owner

Name	Title	Telephone	Email
Gary Noble	CIO	07860 438 776	gary.noble@adept.co.uk

Distribution

Held By	Format	Location	Comments
User	Digital / Physical		

Classification

	Classification
	Confidential
X	Official
	Public

Contents

Objective

The primary objective of our Informational Security Policy is to protect the services to our customers and the data we manage on their behalf as well as protecting the informational asset owned and managed by AdEPT Technology Group plc (hereinafter referred to as AdEPT). It is the company's aim that customers and staff have confidence in our ability to secure their information and have confidence in our ability to respond to security concerns should they arise. Our Information Security Management System (ISMS) policies are based on a formal risk assessment process. Having identified and assessed risks to ourselves and our customers we have selected specific information controls. These controls are summarised in the Statement of Applicability and the policies are available on the company shared area. This policy will apply to all companies within AdEPT that are part of the iso27001:2013 certification.

The Group Leadership Team are committed to meeting the requirements of Information Security best practices and will continue to seek ways in which to improve our security mitigation controls against new or emerging vulnerabilities. We therefore maintain an ISMS which complies with ISO27001:2013. All employees have a role to play in Information Security, it takes a team effort and contribution from all staff to ensure we meet our contractual, statutory, and legal obligations.

The business supports employee's efforts to secure information through continual training and awareness programmes, conducting of internal audits, and monitoring the effectiveness of the policies through performance evaluation and risk assessment as well as carrying out regular Management Reviews on Information Security.

The policies outlined in this document are intended to provide guidelines for managing and addressing Information Security within the Group. The policies are intended to provide direction and support for informational security in accordance with business requirements including relevant laws and regulations.

All policies shall as a minimum:

- Ensure the resources required by Information Security are made available and any training / competency requirements are met
- Ensure a consistent message and approach to Information Security is reflected to the business
- Be based on actual security requirements based on risk assessment, risk treatment and best standards
- Be achievable, measurable and provide outcomes that show effectiveness of the policy
- Identify the roles and responsibilities required to implement and maintain the policies
- Identify internal / external parties that should be engaged where applicable
- Be regularly reviewed and continuously improved to address new vulnerabilities
- ISMS policies have been reviewed and approved by the leadership team

Scope

Within this document we have outlined the Information Security policies which have been implemented to minimise the increasing and wider variety of threats and vulnerabilities associated with information assets. These threats and vulnerabilities have been identified following a formal risk assessment and the policies implemented to address these threats and vulnerabilities which have been developed using ISO27001:2013 best practice guidelines.

The business operates a certified ISMS according to this international standard even if not every process, legal entity or department is part of the scope of the ISMS, the objectives still apply to all of them.

The policies and guidelines are valid and mandatory for all employees and available on the company share drive. All members of staff should both read and adhere to these policies.

The scope is for the provision of integrated and fully managed IT, network and communication solutions, including design, installation management, configuration, testing and in life support, maintenance and management, in accordance with the State of Applicability.

References

ISO 27001:2013 Information Security Management

Distribution

All policies / documents required for Information Security Management shall be protected and controlled. All policies / documents will be:

- Approved for adequacy by the Information Security Committee prior to issue.
- Ensure that all policies / documents are version controlled and the changes / revision status updated
- Ensure that all policies / documents legible and readily identifiable
- Ensure that documents are available to those who need them
- Ensure that any out of date policies / documents are transferred, stored and ultimately disposed of
- Ensure that the distribution of documents is controlled
- Apply suitable identification to them if they are retained for any purpose

Review of Policy

As a minimum this Policy will be subject to joint review on an annual basis unless an earlier date is agreed by the ISO Committee

This policy will also be subject to review / update to respond to any changes in the risk assessment or risk treatment plan and subject to joint review on at least an annual basis

Policy

It is the policy within AdEPT that the information it manages, in both electronic and hard copy, is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. The policy provides management

direction and support for implementing information security across the organisation, in both electronic and hard copy. The specific, subsidiary information security policies should also be considered part of this information Security Management System.

The Information Security policies have been ratified by the Company and form part of its standard operating policies and procedures, including its regulations for Conduct. It is applicable to and is communicated to staff and other relevant parties. This policy will be reviewed every year and updated, as applicable, to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

IT SECURITY

The purpose of this policy is to define a framework on how to protect AdEPT 's computer systems, network and all data contained within, or accessible on or via these computer systems from all threats whether internal, external, deliberate or accidental.

It is the policy of AdEPT to ensure that:

- All central computer systems and information contained within them will be protected against unauthorised access
- Information kept in these systems is managed securely, not only to comply with relevant data protection laws, but also in a professional and dependable manner
- All employees are aware that it is their responsibility to adhere to this policy
- All parties accept total responsibility for maintaining, adhering to and implementing this policy within their areas
- All regulatory and legislative requirements regarding computer security and information confidentiality and integrity will be met by AdEPT
- All breaches of security will be reported to and investigated by a member of the AdEPT IT Team

The Computing Environment

The AdEPT IT Team, plan, maintain and operate a range of central computing servers, core network switches, edge network switches, backup systems, and the overall network infrastructure interconnecting these systems.

The AdEPT IT Team reserves the right to monitor, log, collect and analyze the content of all transmissions on networks and individual departments and organisations at any time deemed necessary for performance and fault diagnostic purposes.

Physical Security

AdEPT IT Team provides a secure machine room with protected power arrangements and climate-controlled environment. Primarily for the provision of central computing and network facilities individual departments.

Any computer equipment in general office environments should be within physically secure rooms outside of general office hours.

Access to Systems

Computer and network systems access is only via individual user accounts. Please refer to the user accounts policy for further details and account eligibility.

Email

Accounts provide access to email facilities. Use of email is governed by the AdEPT Email policy, this can be seen within the staff handbook.

File Storage

All users have access to the centrally managed file storage. Use of the centrally managed file storage is accessed with hierarchical password security.

Internet Access

The AdEPT network is connected to the internet. The AdEPT IT Team operate and maintain a firewall with the aim of protecting the network and computer systems from unauthorised or illegal access or attack from the external environment.

Remote Access to Systems

Remote access is defined as accessing systems from a physically separate network. This may include:

- Connections direct across the Internet
- VPN Connections
- Direct dial connections to the RAS (Remote Access Service)

Any user with a valid AdEPT computer account may access systems as appropriate. Remote access is allowed via secure methods only. Remote connections to any IT services are subject to the same rules and regulations, policies and practices just as if they were physically on any of the AdEPT premises.

The AdEPT IT Team shall provide the only VPN and dial-in service that can be used. All connections via these services will be logged. No other remote access service shall be installed or set up, including single modems connected to servers or workstations. Any active dial-in services found to be in existence will be removed from the network.

Data Security

AdEPT holds a variety of sensitive data including personal information about customers and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

Anti-Virus Security

The AdEPT IT Team will provide means by which all users can download and install current versions of site-licensed virus protection software.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, a complete virus scan should be performed. If the AdEPT IT Team detect a machine behaving abnormally due to a possible viral infection it will disconnected from the network until deemed safe.

DATA PROTECTION

This document sets out the obligations of AdEPT ("the Company") with regard to data protection and the rights of people with whom it works in respect of their personal data under the Data Protection Act 20188 ("the Act") which incorporates the GDPR provisions which are specific to the UK.

This Policy shall set out procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners, or other parties working on behalf of the Company.

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully.

The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply. All personal data:

unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Personal Data

The Company only holds personal data which is directly relevant to its dealings with customers. That data will have been provided to the Company by the customer and be held and processed in accordance with this Policy. The following data or part thereof may be collected, held and processed by the Company from time to time:

- Name
- Address
- Email Address
- Telephone Numbers
- Company Name
- Website Password

Processing Personal Data

Personal data may be disclosed within the Company. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within theCompany that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)
- All personal data is accurate at the time of collection and kept accurate and up to date while it is being held and / or processed
- No personal data is held for any longer than necessary in light of the stated purpose(s)
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data
- All personal data is transferred using secure means, electronically or otherwise No personal data is transferred outside of the Company's operating territory without first ensuring that appropriate safeguards are in place in the destination country or territory

Data Protection Procedures

The Company shall ensure that all its employees, contractors, agents, consultants, partners, or other parties working on behalf of the Company comply with the following when processing and /

or transmitting personal data:

- All emails containing personal data must be encrypted
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient. Using an intermediary is not permitted
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed

Training / support

- This policy will be communicated effectively to all relevant staff working for, or on behalf of AdEPT Technology Group plc
- The policy will also be placed on the AdEPT SharePoint site for staff referral
- One to one training on the Policy will be delivered as a facilitated training session on request

End of Document.