Ahead

MANAGEMENT GROUP

Data Classification Policy

Building fair and effective standards into our business

Table of Contents

AheadMG Ltd 4th Floor, Silverstream House, 45 Fitzroy Street, Fitzrovia, London, W1T 6EB

Management@aheadmg.co.uk

Document Control

Document History

	Author	Version	Description
05/04/2016		V0.1	Template Draft
07/04/2016	Andy Ewell	v0.2	Initial AheadMG Draft
13/06/2016	Andy Ewell	V0.3	Reviewed at board meeting, minor amendments.
16/06/2017	Andy Fox	V1.0	Baselined version
12/09/2018	Tracy Allen	V1.1 (Draft)	Draft - Added Text covering GDPR Updated AheadMG business address.
14/09/2018		V1.1 (Approved)	Latest Updates accepted at Exec Meeting
19/07/2019	Tracy Allen	V1.2 (Draft)	Minor updates for 2019
23/07/2019		V1.2 (Approved)	Latest Updates accepted at Exec Meeting
01/07/2020	Tracy Allen	V1.3 (Draft)	Minor updates for 2020
08/07/2020		V1.3 (Approved)	Latest Updates accepted at Exec Meeting
18/02/2022	Donna Chapman	V1.4	Minor updates for 2022
24/08/2023	Donna Chapman	V1.5	Minor updates for 2023

Signatories

Name	Role	Sign off Date
Andy Ewell	AheadMG Delivery Director	08/07/2020
Neil Hickman	AheadMG Finance Director	08/07/2020

Document Storage

All versions of the policy will be stored on our website https://www.aheadmg.com/new-starters/

Data Classification Policy

Purpose

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to AheadMG, so sensitive corporate and customer data can be secured appropriately.

Scope

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of AheadMG employees, as well as to third-party agents authorised to access the data.

Roles and Responsibilities

Describe the roles and responsibilities associated with the data classification effort. Departments should designate individuals who will be responsible for carrying out the duties associated with each of the roles.

Data owner - The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. The data owner shall address the following:

- **Review and categorisation** - Review and categorise data and information collected by his or her department or division
- **Assignment of data classification labels** - Assign data classification labels based on the data's potential impact level
- **Data compilation** - Ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data
- **Data classification coordination** - Ensure that data shared between departments is consistently classified and protected
- **Data classification compliance** (in conjunction with data custodians) - Ensure that information with high and moderate impact level is secured in accordance with local regulations and guidelines
- **Data access** (in conjunction with data custodians) - Develop data access guidelines for each data classification label

Data custodians - Technicians from the IT department or, in larger organisations, the Information Security office. Data custodians are responsible for maintaining and backing up the systems, databases and servers that store the organisation's data. In addition, this role is responsible for the technical deployment of all of the rules set forth by data owners and for ensuring that the rules applied within systems are working. Some specific data custodian responsibilities include:

- **Access control -** Ensure that proper access controls are implemented, monitored and audited in accordance with the data classification labels assigned by the data owner
- **Audit reports -** Submit an annual report to the data owners that addresses availability, integrity and confidentiality of classified data
- **Data backups -** Perform regular backups of data
- **Data validation -** Periodically validate data integrity
- **Data restoration -** Restore data from backup media

- **Compliance -** Fulfil the data requirements specified in the organisation's security policies, standards and guidelines pertaining to information security and data protection
- **Monitor activity** - Monitor and record data activity, including information on who accessed what data
- **Secure storage** - Encrypt sensitive data at rest while in storage; audit storage area network (SAN) administrator activity and review access logs regularly
- **Data classification compliance** (in conjunction with data owners) - Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines
- **Data access** (in conjunction with data owners) - Develop data access guidelines for each data classification label

Data user - Person, organisation or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorised by the data owner. Data users must use data in a manner consistent with the purpose intended, and comply with this policy and all policies applicable to data use.

Data Classification Procedure

1. Data owners review each piece of data they are responsible for and determine its overall impact level, as follows:
    - If it matches any of the predefined types of restricted information listed in Appendix A, the data owner assigns it an overall impact level of "High."
    - If it does not match any of the predefined types in Appendix A, the data owner should determine its information type and impact levels based on the guidance provided in Sections 5 and 6 of this document. The highest of the three impact levels is the overall impact level
    - If the information type and overall impact level still cannot be determined, the data owner must work with the data custodians to resolve the question

2. The data owner assigns each piece of data a classification label based on the overall impact level:

Overall impact level	Classification label
High	Restricted
Moderate	Confidential
Low	Public

3. The data owner records the classification label and overall impact level for each piece of data in the official data classification table, either in a database or on paper.
4. Data custodians apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the official data classification table.

Data Classification Guideline

Use this table to determine the overall impact level and classification label for many information assets commonly used in AheadMG.

AheadMG Compliance Records			
As part of AheadMG onboarding process, employee and associate vetting takes place. This includes the collection of key information about the information including background checks.			
Information Types			
Compliance Data	Information includes gathering of personal information, including name, address, company data, right to work, criminal records checks, financial and credit checks.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Unauthorised disclosure of compliance information can be seriously detrimental to both AheadMG and the individual interests including breaking Data protection and GDPR regulations. Such unauthorised disclosure will break contract and exposure AheadMG to significant fines/penalties.	Compliance information is collected at the point of verbal offer to an individual. After initial collection data is reviewed on an ad hoc basic (where a change is required – i.e. update of address or annual Sanction check).	Compliance data has to be collected and processed prior to allocation of resource onto AheadMG network or 3rd party client site.
Impact Level	Restricted	Restricted	Moderate
Overall Impact Level	Restricted		
Data Classification Label	Restricted		

Impact Level Determination

Use this table to assess the potential impact to the company of a loss of the confidentiality, integrity or availability of a data asset.

Security Objective	Potential Impact		
	Low	**Moderate**	**High**
Confidentiality. Restrict access to and disclosure of data to authorised users in order to protect personal privacy and secure proprietary information.	Unauthorised disclosure of the information is expected to have **limited** adverse effects on operations, organisational assets, or individuals.	Unauthorised disclosure of the information is expected to have a **serious** adverse effect on operations, organisational assets, or individuals.	Unauthorised disclosure of the information is expected to have a **severe or catastrophic** adverse effect on operations, organisational assets, or individuals.
Integrity. Guard against improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity.	Unauthorised modification or destruction of the information is expected to have a **limited** adverse effect on operations, assets, or individuals.	Unauthorised modification or destruction of the information is expected to have a **serious** adverse effect on operations, assets, or individuals.	Unauthorised modification or destruction of the information is expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals.
Availability. Ensure timely and reliable access to and use of information.	Disruption of access to or use of the information or information system is expected to have a **limited** adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a **serious** adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have **a severe or catastrophic** adverse effect on operations, assets, or individuals.

Use of Emails

Emails are the most common vehicle for transferring and exchanging information internally or with a 3rd party. AheadMG use Outlook to support Email, via Office365 subscriptions. Within Microsoft Outlook, you can mark an outgoing email message or all outgoing email messages as private or confidential, which can remind recipients of keeping that message as private.

How to guide

This must be marked when transferring or including Confidential and Restricted Information.

In addition, the Data Classification (not including Public) should be marked at the start of the email subject line.

Use of Office Products

Data is often recorded and transferred within Office products such as Excel, Work, PowerPoint. It is essential that where non-public data classification is included, such documents should be password protected using the Office suite password functionality.

When sending a password protected document, it is good practice to not include the Password details within the same email/communication. Instead AheadMG employees/associates are encouraged to send password details in a separate and distinct communication – checking carefully that the list of receivers is correct.

Individuals must also follow any client-side processes or procedures in this area, especially around access and confidentiality.

Important – Live Production Access (clients)

AheadMG specialise in Test consultancy within the financial domain. AheadMG should never be provided client-side Production accounts or access to unscrambled test data within Test Environments.

A waiver to the above to cover exceptional circumstances will only be possible via Director level agreement.

Appendix A

Describe the types of information that should automatically be classified as "Restricted" and assigned an impact level of "High." Having this list will make the data classification process easier for data owners.

Types of Information that Must be Classified as "Restricted"

Authentication information

Authentication information is data used to prove the identity of an individual, system or service. Examples include:

- Passwords
- Shared secrets
- Cryptographic private keys
- Hash tables

Invoice and Financial Data

Any information relating to individual employee or 3rd party financial information including:

- Payments in/out
- Invoices in/out
- Rate cards / margins
- Accounting software
- Accounts
- Investment and Banking

Personally Identifiable Information (PII)

Examples of PII include, but are not limited to:

- Name: full name, maiden name, mother's maiden name, or alias
- Personal identification numbers: National Insurance Numbers, passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number
- Personal address information: street address, or email address
- Personal telephone numbers
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting
- Biometric data: retina scans, voice signatures, or facial geometry
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person

The following examples on their own do not constitute PII as more than one person could share these traits. However, when linked or linkable to one of the above examples, the following could be used to identify a specific person:

- Date of birth
- Place of birth
- Business telephone number
- Business mailing or email address
- Race
- Religion
- Geographical indicators
- Employment information
- Medical information
- Education information
- Financial information