Data Classification Policy

From Matchi Wiki

Contents

Introduction

This data classification policy details what precautions to take for protecting data in the Matchi enterprise. This is particularly important, since Matchi's one and only saleable asset is data. A data breach could potentially be disastrous. This policy applies to all forms of data storage, data transport and everyone in the business.

All data must have an owner who is responsible for understanding the appropriate risks and implications of the owned data going awry. The data owner is responsible for assigning the classification level of the data and must ensure that it is consistently protected throughout its life cycle up to the point of where the data is destroyed: Data must be protected in a manner commensurate with its sensitivity, regardless of where the data resides, what electronic or printed form it is in, and what technology is used to handle the data.

Although we are not yet subject to strict regulatory compliance (PCI-DSS, Data Protection Act, etc..), our customers have a reasonable expectation that their contact and product details are treated with the utmost respect.

Data Classifications

Public

Description: This data may be freely disseminated outside the organisation without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Accessible by: Available to the general public and for distribution outside of Matchi.

Data Breach Impact: None.

Data Transfer Policy:

- Network: No special handling required
- Email to External accounts: No special handling required
- Email to Internal accounts: No special handling required
- Transfer via removable storage devices: No special handling required

Storage:

- All electronic data: No special handling required
- Printed material: No special handling required

Data Disposal:

- All electronic data: No special handling required
- Printed material: No special handling required

Internal

Description: This classification applies to all other data that does not clearly fit into the other classifications.

Accessible by: Intended for use only within Matchi.

Data Breach Impact: Unauthorised disclosure, modification or destruction of this data is not expected to seriously or adversely impact the organisation, its employees, or its business partners. Examples include the company telephone directory, new employee training materials, and internal policy manuals.

Data Transfer Policy:

- Network: No special handling required
- Email to External accounts: No special handling required
- Email to Internal accounts: No special handling required
- Transfer via removable storage devices: No special handling required

Storage:

- All electronic data: Reasonable precautions to restrict access to internal staff
- Printed material: No special handling required

Data Disposal:

- All electronic data: No special handling required
- Printed material: Paper shredding. Paper recyling allowed.

Confidential

Description: This classification applies to data that is intended solely for use within Tesco. Data that is considered private is included in this classification, as well as data covered by data protection legislation and Payment Card Industry standards.

Accessible by: Access should be limited to a need to know basis as required by staff to do their job, and would not be released externally except for regulatory or legal compliance.

Data Breach Impact: Unauthorised disclosure could adversely impact the organisation, its employees and business partners. Examples include employee Human Resources data, source code, design specification documents, financial data, purchasing data, vendor contracts, and customer data in bulk.

Data Transfer Policy:

- Network: SSH or SSL-encrypted channel
- Email to External accounts: Should only be emailed externally on a need to know basis
- Email to Internal accounts: No special handling required
- Transfer via removable storage devices: Access to the storage device should be password-protected

Storage:

- Active electronic data: Processing systems must be resistant to unauthorised access
- Vaulted electronic data: In a lockable enclosure
- Printed material: In a lockable enclosure

Data Disposal:

- All electronic data: Secure deletion process such as DBAN.
- Printed material: Paper shredding. Paper recyling allowed.

Secret

Description: This classification applies to the most sensitive business data that is intended strictly for use within the organisation.

Accessible by: Access is limited to as few persons as possible and on a need to know basis. As this data is very sensitive it should be closely controlled from creation to destruction.

Data Breach Impact: Unauthorised disclosure could seriously and adversely impact the organisation, its shareholders, employees and its business partners. Examples include merger and acquisition documents, corporate level strategic plans, and litigation strategy, HR issues, etc.

Data Transfer Policy:

- Network: SSH or SSL-encrypted channel
- Email to External accounts: Data must be in an encrypted file
- Email to Internal accounts: Should only be emailed externally on a need to know basis
- Transfer via removable storage devices: Must be encrypted

Storage:

- Active electronic data: There should not be any secret data on any processing systems
- Vaulted electronic data: In a lockable enclosure
- Printed material: In a lockable enclosure

Data Disposal:

- All electronic data: Secure deletion process such as DBAN.
- Printed material: Paper shredding and incineration.