Kimcell Group

DATA QUALITY POLICY

Author: Doina Savu

Table of Contents

1. Scope

1.1. Kimcell's Information Security Policy sets out the minimum policy standards for confidentiality, integrity and availability of information. It covers the overlapping areas of data protection, compliance, information security, data quality and confidentiality.

1.2. The purpose of this data quality policy is to build on the guidance contained within the Information Security Policy and provide specific guidance for maintaining and increasing the levels of data quality within Kimcell Ltd.

2. Domain

2.1. This policy covers all types of data collected and recorded within the company. As the data produced is generated to provide information for a variety of uses, a true definition of "data quality" cannot be easily found. The emphasis is therefore is on completeness, accuracy, timeliness and compatibility of data items.

3. Legal Framework

3.1. The main relevant legislation regarding the collections and use of data is:

3.1.1. Data Protection Act 1988

3.1.2. Freedom of Information Act 2000

3.1.3. Human rights Act 1998

3.1.4. Computer misuse Act 1990

4. Policy Statements

4.1. Data quality relates to the accuracy of data used to judge performance or inform business decisions. This can include information collected from processes or systems, performance indicator results, information about key actions and projects or information required for the domain registration process.

4.2. Producing information that is fit for purpose should not be an end in itself, but an integral part of the organisation's operations, performance management and governance arrangements

4.3. Kimcell Ltd. is committed to excellent data quality in all of the information used to assess performance. This is particularly important because:

4.3.1. It supports continuous improvement and more effective use of resources;

4.3.2. Good data quality is crucial to support effective decision making – not just in terms of performance management, but also business and strategic planning

4.3.3. It contributes to the provision of high quality information to our customers, suppliers, certification bodies and partners

4.3.4. It allows interested parties to make objective judgements about the quality of the services Kimcell Ltd. delivers and can aid effective benchmarking

5. Data quality requirements

5.1. Validity

5.1.1. All data held on Kimcell's information systems must be valid. Where codes are used, these will comply with the national standard or will map to national definitions, where available. Wherever possible, systems will be configured to accept only valid data formats

5.1.2. It's also important to validate the source of data/information and where possible, show that such data has come from a verifiable document, report, website system or data repository

5.2. Completeness

5.2.1. All mandatory data items within a data set should be complete. Use of mitigating default codes should only be used where appropriate, and not as a substitute for real data. If a data field is left unfilled due to insurmountable circumstances, than that data should be rectified up as soon as practicable.

5.3. Consistency

5.3.1. Correct procedures are essential to ensure complete and consistent data capture

5.4. Coverage

5.4.1. This reflects all information that is "owned" by Kimcell Ltd, including paper and computerised records

5.5. Accuracy

5.5.1. Data should be sufficiently accurate for its intended purposes and presented clearly in the appropriate level of detail. Accuracy is more likely to be achieved if data is collected as close as possible to the point of service delivery.

5.6. Timeliness

5.6.1. Data should be captured as quickly as possible to ensure it is available for review within a reasonable time period. Data must be available quickly and frequently enough to support effective performance management and to allow corrective action to be taken before a service period ends.

5.7. Accessibility

5.7.1. All relevant data and information should be accessible to users via on-line information systems – and as soon as it becomes available

6. Validation methods for domain registration

6.1. Kimcell Ltd. uses the MangoDomains database to record all relevant domain information This database works to ensures all necessary information is captured and the collective data fields serve as a check and balance, endeavouring to ensure data is valid and relevant.

6.2. This policy aims to satisfy the requirements of data validation for domain registration. The following represent valid data for this purpose:

6.2.1. Section 1 – Address Format

6.2.1.1. Street 1 contains Alpha Numeric information

6.2.1.2. Post Town

6.2.1.3. Country

6.2.1.4. Post Code for UK

6.2.1.5. Post Code applicable to non- UK addresses

6.2.2. Section 2 – Phone numbers Format

6.2.2.1. begin with a "+"

6.2.2.2. Followed with a country code

6.2.2.3. Digits after country code

6.2.3. Section 3 – E-mail Format

6.2.3.1. contains an'@'

6.2.3.2. ends with a valid TLD (Top Level Domain)

6.2.3.3. Contains at least one character before the "@"

6.2.3.4. must not have any trailing or leading spaces

6.2.4. Section 4 – Correct Use of Trading Name Field (trad-name)

6.2.4.1. Trading Name Field (trad-name) should be used by sole traders for their business name. Organisation name field to

6.3. If after submitting data to the Registrar, this is returned as invalid, the following actions should be taken:

6.3.1. An engineer should verify if the data submitted for validation is the same as data kept in MangoDomains.

6.3.2. If the data corresponds, contact shall be made with the Registrant of the domain to determine if the details held are still acurate. If they are then proceed to 6.3.3.

6.3.3. In some cases, even if the data submitted is correct, the registrar might still respond with an invalid request due to the fact that the details do not appear on public data sources available to the registrar. In this case, documentation will need to be provided to the Registrar, such as copy of official ID, incorporation certificate, etc. If this is the case, the Registrar will validate the data

6.3.4. If after providing the Registrar with the Registrant's validation documents, the former still cannot validate the domain, but our company is happy that the details are valid and correct, then no further action is needed as the company can take responsibility for the validation of the details provided by the registrant

6.3.5. If for any reasons, we are unable to validate the data submitted to the Registrar, than the domain will be suspended until correct validation information is received.

7. Compliance

7.1. Information Security auditing will conduct regular monitoring to enforce compliance with this policy. Any violation of this policy will be investigated and if found to be caused by wilful disregard or negligence, will be treated as a disciplinary offence. All disciplinary proceedings are coordinated

7.2. Kimcell Ltd. reserves the right to amend this policy at any time and will publish updated versions to all staff.

APPROVED	**CREATOR**
DIRECTOR	COMPLIANCE MANAGER
TIM HARRIS	DOINA SAVU