SECPOL02 – Data classification and handling policy

Version:	1.0
Last Review Date:	26/10/2023
Reviewed By:	Lisa Brockman. National Gas Security GRC – Policy and Assurance
Approved By:	Polly Cameron. National Gas Chief Information Security Officer
Next Review Date:	26/10/2024
Contact:	box.SecurityGRC-PolicyAndAssurance@nationalgas.com
Latest Version	The latest version of this policy is available on the National Gas Security GRC public SharePoint site.

Contents

1. Introduction

1.1. Overview

Data fuels our business, and the ability to access secure, accurate data when it is required is critical to the success of National Gas. However, not all our data is equal, and it exists in many forms (digital and physical).

To help us distinguish and identify the importance of our data, we need to have a set of principles and practices to classify our information to drive consistent behaviours and controls across National Gas. In applying these behaviours, we ensure appropriate protections are in place to defend against internal and external threats, whether accidental or malicious.

1.2. Purpose

The purpose of this policy is to provide the classification and handling requirements for National Gas data.

1.3. Scope

- All National Gas entities
- All National Gas employees, contractors, and suppliers who access National Gas data and information
- All National Gas data and information that is created, collected, stored, processed, or transmitted in electronic and non-electronic formats.

1.4. Intended audience

All National Gas employees, contractors and suppliers owning, operating, creating, storing, transmitting, or accessing National Gas data or information.

1.5. Legal and regulatory

This policy aligns with statutory and regulatory requirements in place on the date it was approved. Appendix A lists the relevant regulations and versions.

1.6. Further information

Further information on our Information Security Management System (ISMS) is available on the National Gas Security GRC SharePoint, including document maintenance, review, feedback, the update and approval process, and continual improvement. You can also find details of how we measure compliance, non-compliance and manage exceptions.

1.7. Guidance and support

For guidance on how to comply with this policy, refer to the National Gas Security GRC public SharePoint site or contact the National Gas Security GRC Policy and Assurance Team via **box.SecurityGRC-PolicyAndAssurance@nationalgas.com**.

2. Security classification

All data created within National Gas requires a security classification:

Classification	Characteristics	Examples
Official	• This is our base classification for data in National Gas and is characterised as data that is **not intended for public release** and is intended to be shared with **named individuals** who have a business need to access it. • In addition, the data contains no personal, commercial, or sensitive information, • A compromise **could** cause no more than **moderate damage** to the work or reputation of National Gas.	Meeting packs, minutes, actions, policies, procedures, internal reports.
Official – For public release	• Where there is a business need, National Gas "Official" data may also be distributed outside of the company, for example press releases or bulletins and reports for the general public. In these cases, your data should be labelled as "Official – for public release".	Press releases or bulletins and reports for the general public.
Official – Sensitive	• This type of data is of at least some interest to threat actors (internal or external), activists or the media. • Official company data that is **not intended for public release** and is intended to be shared with **named individuals** within the company. • A compromise **is likely to** cause **moderate** damage to the work or reputation of National Gas.	Audit reports, site drawings, security information, configuration details.
Official – Sensitive personal	• Official company data containing Personally Identifiable Information (PII) or Sensitive Personal Information (SPI). That is, data relating to an identified or identifiable living individual. • This type of data is **not intended for public release** or full company release and is intended to be shared with **named individuals** who have a business need to access it. • This data is protected under the UK Data Protection Act and the General Data Protection Regulation, or GDPR and must be protected to ensure it is stored and shared correctly.	Documents containing date of birth, address, employee performance reports, health information.
Official – Sensitive commercial	• Data that may be commercially damaging to National Gas or to a commercial partner if improperly accessed, or which is subject to terms of commercial confidentiality.	Contracts, Intellectual property designs and plans

Note: The National Gas security classification schema is aligned with the UK Government Security Classifications Policy.

3. Structured and unstructured data

National Gas holds data in both structured and unstructured formats and can be digital (such as office documents, online applications, and services), or analog (such as letters, printed documents or books).

3.1. Unstructured data

Unstructured Data is data that is created by National Gas employees, contractors and third parties as part of their daily activities, where there is no existing reference classification to refer to.

Security controls embedded in enterprise Technology services such as email and information sharing, and storage solutions will protect the data based on the selected security classification.

Examples of unstructured data are slide packs, emails, and meeting minutes.

The requirements for handling Unstructured Data are in *Section 4* of this document.

3.2. Structured data

Structured Data is data that adheres to a pre-defined data model and is stored and managed consistently. (A data model is a model that organises elements of data together and standardises how they relate to one another).

Examples of structured data are National Gas Approved File Sharing Services, databases and applications. These data types are usually managed by our Technology team, and not by individual National Gas colleagues.

The requirements for handling Structured Data are in *Section 5* of this document.

3.3. Is my data structured or unstructured?

Unless you are working in Technology, or are a System, Application or Product Owner – your data is most likely to be unstructured. If you are unsure, please reach out to the National Gas Security GRC Policy and Assurance Team via box.SecurityGRC-PolicyAndAssurance@nationalgas.com.

4. Policy statement – unstructured data

4.1. Classifying new unstructured data

Creating a new item of data requires:

- An author (typically the person who created it)
- An owner (the person who is accountable for the data). The owner to determine the appropriate security classification (using the criteria detailed in Section 3) for the new asset.

Note: Any new data asset created from an existing data asset should inherit the classification rating if the content remains the same. If the content of the data is significantly changed, or further content added, the classification must be reviewed in line with this policy.

4.2. Marking/labelling

Once the classification has been selected, the asset must be clearly marked to indicate the Security Classification.

- Documents stored in digital form must include their classification rating using the footnote section of each page.
- Email communications must include the classification assigned to the content in the email body (e.g as part of the senders' signature).
- Paper information must include its classification rating clearly on each page.

Note: Any unmarked documents will be treated as Official.

4.3. Handling

Data must be handled as per *SECSTD02 – Data classification and handling standard.*

4.4. Data access

Data must only be shared using a least privilege model, with only those who have a business need to the data having permission to access it.

The access granted to data must be granted and reviewed as per *SECPOL03 – Access Control*.

4.5. Aggregated data

Consideration must be given to aggregated data sets. You must ensure segregation of data is maintained in line with segregation of duties to mitigate the likelihood that a single point of compromise could have a significant impact on National Gas.

5. Policy statement - handling structured data

This section is for Application Owners, Product Owners, and IT Teams who own, operate, or manage structured data on behalf of National Gas.

5.1. Identifying your data

Identifying and understanding the characteristics of the data that is to be handled is vital to ensure it can be classified correctly, and that appropriate security controls are applied to protect it. This section aims to establish a clear, repeatable set of actions that must be taken for all new structured data within National Gas

5.2. Strategic importance/business criticality classification

All data must have a Business Criticality Classification based on the Strategic Importance of the data:

Classification	Definition
Operationally Critical [1]	Data that is deemed essential to the continuance and delivery of a set of activities / processes that are deemed essential to delivering the primary objective of the day-to-day operation and control of National Gas.
Critical [1]	Data that is deemed essential to the continuance and delivery of activities / processes that are deemed critical to maintaining legal, regulatory, commercial, and business responsibilities.
Core	Data that is deemed essential to the continuance and delivery of any activity / process that is central to National Gas' normal day-to-day activities. Such data would affect the ability of National Gas to manage its businesses effectively with consequential impacts on business profitability and reputation.
Efficiency and Performance	Data that if incomplete, inaccurate, or missing is unlikely to have a significant impact on the public or the business in the short to medium term but may impact on the efficiency and performance of National Gas over time.

[1] Business critical data and critical data elements must be classified as either Operationally Critical or Critical.

5.3. Data asset register

A Data asset register must be in place which contains a record of all data assets with a Strategic Importance Business Criticality of Core, Critical and Operationally Critical (as per section 5.2).

The register must:

- identify the characteristics of data being classified
- identify the Owner of the data
- contain the Strategic Importance/Business Criticality Classification
- contain the Regulatory Classification
- contain the Security Confidentiality Classification
- identify if the data contains Personally Identifiable Information (PII) or Sensitive Personal Information (SPI)
- be reviewed annually, or when a change has occurred, to ensure it is accurate
- document the users who have access to the data
- document the location, quantity, and quality of the data. (This information would be linked to the Data Asset Register and stored in the Service Management Tooling to provide accuracy and timeliness to this information).

5.4. Assessing requirements

National Gas has three security objectives that must be considered when determining the level of security controls to apply to a new set of data.

Confidentiality	Only authorised people have access to the data.
Integrity	The data has not been altered or destroyed by an unauthorised person or process.
Availability	The data is available when it is needed.

Note regarding Availability:

To prevent conflicting requirements, availability is not part of the Security Classification process. All availability requirements must be determined as part of the IT Service Introduction process based on the business requirement for the data.

5.5. Introducing new data sets

Each new data set:

- must go through an assessment to determine the appropriate Security Confidentiality Classification rating and associated Integrity rating.
  The resulting Security Confidentiality and Integrity ratings must be recorded in the Data Asset Register. **Note:** The associated Integrity rating must not be changed and must be as per the table above in this section.
- must have its classification reviewed if:
  - Data attributes have changed significantly (e.g anonymisation).
  - The value of the data (impact) has changed (e.g. financial results prior to publication versus after they have been published).
  - The annual assessment is due.
- must be clearly labelled with its assigned classification rating.
- must inherit the classification rating of the source if an exact copy.

5.6. Security control selection

Security Controls are the safeguards agreed by National Gas to protect the Confidentiality, Integrity and Availability of the data that is processed, stored, or transmitted by our systems. Further information on the required controls is available in *SECSTD02 – Data classification and handling standard*.

5.7. Security control implementation

- All National Gas data systems must apply Security Controls appropriate for the protection of the data the system processes, stores and/or transmits.
- The Security Controls applied to Systems and Sub System Components must be selected to meet the **highest classification** of data to be processed, stored, or transmitted by the system.
- The selection of Security Controls must satisfy the requirements set in relevant *National Gas Policies and Standards*.
- Selection of Security Controls must align with the type and role of the information system. (e.g. At rest (storage) related controls don't apply to a system that only transmits or processes data).
- Should a perceived conflict of security control requirements be identified the higher requirement must take precedence.

5.8. Data backups

- Company information must be backed up, retained, and tested in line with the *SECPOL08 – Backup Policy*.

6. Controls

The following table shows the controls in place for this policy:

Control Ref	Control Type	Title	Description
CIS IG1 3.1	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
CIS IG1 3.2	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.
CIS IG1 3.3	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
CIS IG1 3.4	Protect	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.
CIS IG1 3.5	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
CIS IG1 11.3	Protect	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

7. Appendices

7.1. Appendix A: Regulatory and compliance requirements

We have designed this policy to meet the following regulatory and compliance requirements:

- **Regulations**
  - *Network and Information Security 2 2022/2555 Directive*
  - *Data Protection Act 2018 (DPA 2018) and UK GDPR (General Data Protection Regulation)*
- **Standards**
  - *ISO 27001:2022*
  - *ISO 27019:2017*
  - *IEC 62443*
- **Frameworks**
  - *NCSC Cyber Assessment Framework (CAF) v3.1*
  - *NIST Cyber Security Framework v1.1*
  - *CIS Critical Security Controls v8*

7.2. Appendix B: Other relevant documents

Documents are available on the *National Gas Security GRC public SharePoint site*.

- *SECSTD02 – Data classification and handling standard*
- *SECPOL03 – Access Control*
- *SECPOL08 – Backup Policy*

7.3. Appendix C: Document version history

Version	Date	Author	Changes
0.1	13/06/2023	Lisa Brockman	Initial Draft
0.2	22/06/2023	Lisa Brockman	Updated with comments post feedback
0.3	27/06/2023	Lisa Brockman	Updated post feedback
0.4	27/07/2023	Adnan Taj	Updated post feedback, changes to structure and addition of summary tables.
0.5	31/07/2023	Lisa Brockman	Updated post feedback
0.6	06/09/2023	Adnan Taj	Updating Policy
0.7	18/10/2023	Lisa Brockman	Revised formatting and layout to align with new classification scheme
0.8	23/10/2023	Lisa Brockman	Updated post feedback
1.0	26/10/2023	Lisa Brockman	Approved version