|  |  |
| --- | --- |
| **Title** | Data Sensitivity Classification Policy |
| **Owner** |  |
| **Version Number** |  |
| **Document Id** |  |
| **Primary Audience** |  |
| **Document Location** |  |
| **Next Review Date** |  |

# Objective

This policy sets out the data sensitivity classifications and corresponding minimum standards for handling data. Its purpose is to protect the information we hold from unauthorised access, modification, and distribution, whether through an inadvertent act or a deliberate attack from an adversary.

# CONTEXT

## Business Context

This sensitive data classification policy details the precautions to protect data within the Succession Group and the customer's enterprise. It applies to all data storage and transport forms and everyone in the business.

## Regulatory Context

Succession’s requirements for meeting its obligations under the UK General Data Protection Regulation as well as the FCA’s expectations regarding how it collects, manages, secures and disposes of client data according to the sensitivity of the data, are set out in the Data Protection and Privacy Policy.

## Scope

This policy covers the entire life cycle of data within Succession. It includes all written and electronic information held, used or transmitted by or on behalf of Succession, in whatever media. This also includes information on computer systems, hand-held devices, phones and paper records.

The information covered by this policy includes:

* personal information relating to staff, clients, and suppliers.
* other business information; and
* confidential information.

Information Security is everyone’s responsibility, so this Policy applies to all staff, including employees, self-employed planners, contractors, interns, volunteers and apprentices. In addition, where appropriate, the requirements of this Policy should be communicated to all third parties who are or will be processing information on our behalf, so they can ensure that their systems and controls reflect the minimum standards set out in this Policy.

## Risk Appetite Alignment

The nature of information and cyber security risks is such that they can never be fully mitigated. However, the Boards have no appetite for unauthorised or inappropriate transport, processing or release of data held by the Succession Group or our third parties.

# REQUIREMENTS

## Roles & Responsibilities

**The Data Owner is responsible for:**

All data must have an owner responsible for understanding the appropriate risks and implications of the owned data getting breached. The Data Owner is also responsible for assigning the data sensitivity classification of the data and must ensure that it is consistently protected throughout its life cycle up to destruction in a manner commensurate with its sensitivity, regardless of the type of media that the data resides on and what technology is used to handle the data.

**All Staff are responsible for:**

* Understanding their responsibilities for ensuring that sensitive data is correctly classified and treated according to the classifications.
* Line managers must ensure their team members know their responsibilities within this policy.

**The Group Data Architecture Team is responsible for:**

* Ensuring that all data has an assigned responsible data owner and a data steward
* Ensuring that the roles and responsibilities of the Data Owner and Data Steward are understood
* The correct processes for storage, transmission and use are followed during the data’s life cycle
* Report data breaches to the Group Risk Committee

**The Group Executive and Boards are responsible for:**

* Ensuring that the business is appropriately resourced to implement the processes set out in this policy.

**The Group Risk Committee is responsible for:**

* Reviewing the effectiveness of arrangements to identify and manage sensitive data classifications as determined by data owners
* Reviewing and challenging reports on sensitive data security breaches and proposed actions to address these breaches and to prevent recurrence.

**The Director of Technology, assisted by the Succession Technology team is responsible for:**

* Providing the Group Executive and Boards with reports on data breaches

**Third Parties are responsible for:**

* Adhering to these prescribed storage, transmission and processing measures based on the sensitivity classification of data owned by the Succession Group.

## Policy Application

Refer to the Policy Application in the document [Information Security Policy](https://successiongroup.sharepoint.com/:w:/r/sites/CyberProject/Shared%20Documents/X%20Archive/Information%20Security%20Policy.docx?d=w9fa0eb691ad34278bc537a8860a906ad&csf=1&web=1&e=F1OAOC) [Ref. 1].

## Monitoring, Testing, Reporting, and Measurement of Effectiveness

Assurance activity will be undertaken by Risk & Compliance and /or by appropriately qualified third parties. The results of assurance activities will be shared with the Executive and, where appropriate, Boards and the Group Risk Committee.

Effectiveness will be measured through:

* Regular first line monitoring of adherence to the Policy and Framework.
* Regular review of MI by the Boards, Executive Committee, and Group Risk committee.
* The review of any risk events, service and performance issues about information security arrangements by the Group Risk Committee and other relevant forums will be used to consider any changes to the controls, Policy and/or Framework.
* Ensuring a continuous yearly Cyber Essentials accreditation to maintain and improve cyber security encompassing infrastructure, systems and remote working to mitigate the risk from common cyber threats

## Breaches

Any Breach of this policy will be treated as serious and may result in disciplinary action. Breaches of the policy must be reported following the Risk Event reporting process.

# DATA CLASSIFICATIONS

## Classification: Public Data

|  |
| --- |
| **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 the Succession Group  **Data Breach Impact:**  None.  **Network Data Transfer Policy:**   * 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 digital data: No special handling required * Printed material: No special handling required   **Data Disposal:**   * All digital data: No special handling required * Printed material: No special handling required |

## Internal Data

|  |
| --- |
| **Description:**  This classification applies to all other data that does not fit into the other classifications.  **Accessible by:**  Intended for use only within the Succession Group.  **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.  **Network 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 digital data: Reasonable precautions to restrict access to internal staff * Printed material: No special handling required   **Data Disposal:**   * All digital data: No special handling required * Printed material: Paper shredding. Paper recycling is allowed. |

## Confidential Data

|  |
| --- |
| **Description:**  This classification applies to data that is intended solely for use within the Succession Group. Data 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.  **Network Data Transfer Policy:**   * SSH or SSL-encrypted channel * Email to External accounts: Should only be emailed externally on a need-to-know basis * Email to Internal accounts: Email should be marked as Confidential.   **Transfer via removable storage devices:**   * Access to the storage device should be password-protected   **Storage:**   * In-use digital data: Processing systems must be protected from unauthorised access * Vaulted electronic data: In a lockable enclosure * Printed material: In a lockable enclosure   **Data Disposal:**   * All digital data: Secure deletion process such as DBAN. * Printed material: Paper shredding. Paper recycling is allowed. |

## Secret Data

|  |
| --- |
| **Description:**  This classification applies to the most sensitive business data 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 trade secrets, merger and acquisition documents, corporate-level strategic plans, litigation strategy, HR issues, etc.  **Network Data Transfer Policy:**   * File transfer over a temporary SSH or SSL-encrypted channel custom-made for the sender and recipient for the duration of the file transmission * Email to External accounts: Data must be in an encrypted file on a need-to-know basis * Email to Internal accounts: Should not be emailed externally   **Transfer via removable storage devices:**   * Files containing this classification of data must be encrypted * The encryption key and storage device must be handed over to the recipient via two different transfer modes.   **Storage:**   * Active digital data: There should not be any secret data on any processing systems * Vaulted digital data: In a lockable enclosure * Printed material: In a lockable enclosure   **Data Disposal:**   * All digital data: Secure deletion process such as DBAN. * Printed material: Paper shredding and destruction. Paper recycling is not allowed. |

# CONTACT FOR QUERIES AND GUIDANCE ABOUT THIS POLICY

Queries are to be initially addressed to the IT Service Operations team.

**POLICY**

**SUPPORTING & REFERENCE MATERIALS**

|  |  |  |  |
| --- | --- | --- | --- |
| SUPPORTING & REFERENCE MATERIALS | | | |
| **Ref** | **Title** | **Document Id** |
| 1 | Information Security Policy |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| REVIEW AND APPROVAL OF POLICY | | |
| **Reviewed by** | **Job Title/Role** | **Date** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Approved by** | **Job Title/Role** | **Approval Date** |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| HISTORY AND VERSION CONTROL | | | |
| **Version #** | **Author** | **Comments** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |