

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.



Smart Energy Code

# Panel Information Policy

---

**Version 6.1**

5 March 2025

## Change Record

| VERSION | STATUS | ISSUE DATE | AUTHOR | COMMENTS                                                                        |
|---------|--------|------------|--------|---------------------------------------------------------------------------------|
| 0.1     | Draft  | 08/05/2015 | SECAS  | Initial Draft release                                                           |
| 0.2     | Draft  | 07/08/2015 | SECAS  | Updated Initial Draft                                                           |
| 0.3     | Draft  | 08/04/2016 | SECAS  | Updated following SEC contribution consultation                                 |
| 1.0     | Final  | 26/05/2016 | SECAS  | Final Document for Publication                                                  |
| 1.1     | Draft  | 07/09/2016 | SECAS  | Initial Draft release for SSC review                                            |
| 1.2     | Draft  | 30/09/2016 | SECAS  | Amended following comments received from SSC, the DCC, and the SSC Chair        |
| 1.3     | Draft  | 04/11/2016 | SECAS  | Amendments following comments received from TABASC Chair, SSC Chair and the DCC |
| 2.0     | Final  | 16/11/2016 | SECAS  | Final Document for Publication                                                  |
| 2.1     | Final  | 09/12/2016 | SECAS  | Amended wording for RED classification level                                    |
| 3.0     | Final  | 10/02/2017 | SECAS  | Amended following legal review                                                  |
| 3.1     | Draft  | 08/03/2019 | SECAS  | Additional wording following request by the SECCo Board                         |
| 4.0     | Final  | 15/03/2019 | SECAS  | Final Document for Publication                                                  |
| 5.0     | Final  | 09/12/2022 | SECAS  | Final Document for Publication                                                  |
| 6.0     | Final  | 03/07/2023 | SECAS  | Amend classifications and descriptions in line with FIRST standard change       |
| 6.1     | Final  | 05/03/2025 | SECAS  | Annual review Minor revisions to examples and added meeting recording guidance  |

## Document Controls

| REVIEWER  | ROLE              | RESPONSIBILITY                 | DATE                           |
|-----------|-------------------|--------------------------------|--------------------------------|
| SEC Panel | Document Approver | Panel Information Policy Owner | 20 <sup>th</sup> May 2016      |
| SEC Panel | Document Approver | Panel Information Policy Owner | 11 <sup>th</sup> November 2016 |
| SEC Panel | Document Approver | Panel Information Policy Owner | 15 <sup>th</sup> March 2019    |
| SEC Panel | Document Approver | Panel Information Policy Owner | 27 <sup>th</sup> June 2023     |
| SEC Panel | Document Approver | Panel Information Policy Owner | 5 <sup>th</sup> March 2025     |

Date of next review: 04/12/2025

## Contents

|                                                               |           |
|---------------------------------------------------------------|-----------|
| 1. Purpose .....                                              | 5         |
| 2. Scope .....                                                | 5         |
| 3. Data.....                                                  | 5         |
| 4. Principles.....                                            | 6         |
| 5. Governing the Panel Information Policy.....                | 6         |
| <b>5.1 SEC Party responsibilities.....</b>                    | <b>6</b>  |
| <b>5.2 SEC Panel and Sub-Committee responsibilities .....</b> | <b>7</b>  |
| <b>5.3 SECAS responsibilities.....</b>                        | <b>7</b>  |
| 6. Handling, labelling, and storing confidential Data .....   | 7         |
| <b>6.1 Confidential data .....</b>                            | <b>7</b>  |
| <b>6.2 Labelling .....</b>                                    | <b>8</b>  |
| <b>6.3 Handling .....</b>                                     | <b>8</b>  |
| <b>6.4 Storage .....</b>                                      | <b>9</b>  |
| <b>6.5 Retention .....</b>                                    | <b>9</b>  |
| <b>6.6 Confidentiality and Disclosure Agreement .....</b>     | <b>10</b> |
| <b>6.7 Secure paper platforms .....</b>                       | <b>10</b> |
| <b>6.8 Downgrading papers .....</b>                           | <b>11</b> |
| <b>Appendix A DCC Classifications .....</b>                   | <b>12</b> |
| 1. Classifications .....                                      | 12        |
| <b>1.1 DCC Confidential .....</b>                             | <b>12</b> |
| <b>1.2 DCC Controlled .....</b>                               | <b>12</b> |
| <b>1.3 DCC Controlled – SEC Parties .....</b>                 | <b>13</b> |
| <b>1.4 DCC Public .....</b>                                   | <b>13</b> |
| <b>1.5 Unmarked.....</b>                                      | <b>14</b> |
| <b>1.6 Restrictions.....</b>                                  | <b>14</b> |
| 2. Distribution and Receipt of DCC Data.....                  | 14        |
| <b>2.1 Receiving Confidential DCC Data .....</b>              | <b>14</b> |
| <b>2.2 Receiving Controlled DCC Data .....</b>                | <b>15</b> |
| <b>Appendix B: SEC Governance Classifications .....</b>       | <b>16</b> |
| <b>Appendix C: Artefacts Matrix.....</b>                      | <b>20</b> |

## 1. Purpose

SEC Section M4.13 requires that the Panel shall establish and maintain a policy for classifying, labelling, handling and storing Party Data received by it (and its Sub-Committees and Working Groups, SECAS and SECCo) pursuant to the provisions of SEC Section G (Security), SEC Section I (Data Privacy), and SEC Section L (Smart Metering Key Infrastructure) and its related SEC Subsidiary Documents. This document fulfils this obligation and the classification scheme set out within is known as the Panel Information Policy.

The Panel Information Policy provides a framework to which the Panel, its Sub-Committees, Working Groups, SECCo and the Smart Energy Code Administrator and Secretariat (SECAS) shall adhere to in order to safeguard the privacy and security of Party Data handled by them. It describes the classification levels available to SEC Parties in accordance with SEC Section M4, as well as describing how the Panel (and its Sub-Committees and Working Groups, SECAS and SECCo) will handle, store and retain Party Data marked as confidential.

Words and expressions used in this Policy shall be interpreted in accordance with the Smart Energy Code.

## 2. Scope

The scope of this document has been voluntarily expanded to cover all Party Data (not just that received pursuant to the provisions in SEC Sections G, I and L), including that shared orally or visually.

It has also been expanded to include other information which may be of use to SEC Parties.

- Appendix A of this document details the classifications applicable to DCC documents, and SEC Parties should refer to Appendix A if they are in receipt of classified DCC information.
- Appendix B explains the classifications applicable to the Panel, its Sub-Committees, Working Groups, SECCo, the Smart Energy Code Administrator and Secretariat (SECAS), including distribution rules.
- Appendix C provides a list of common artefacts and how they are classified.

## 3. Data

The content of this Policy applies in respect of the Data (other than SEC Materials and Consumer Data) that is provided (or otherwise made available) pursuant to the Code or to the Panel (or its Sub-Committees and/or Working Groups, including via SECAS or SECCo) by or on behalf of a SEC Party (such Data being the “Party Data” of that SEC Party).

Data is defined as any information, data, knowledge, figures, methodologies, minutes, meeting recordings/transcripts, reports, diagrams, project artefacts, forecasts, communication messages, images or sounds – such as video or audio recordings (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).

In summary, this document defines the Code classifications available to SEC Parties for classifying Data and how the Panel (and its Sub-Committees and Working Groups, SECAS and SECCo) will label, handle, safeguard and store Data. It also includes information about DCC classifications and how they correspond to SEC classifications.

## 4. Principles

This Panel Information Policy is underpinned by the following principles:

1. Party Data will only be requested by the Panel, its Sub-Committees, Working Groups - including via SECAS or SECCo - where circumstances dictate it is required for the proper performance of their respective duties and functions under the Code (SEC Section M4.7);
2. Party Data categorised as 'confidential' will not be disclosed, or access be authorised, where that SEC Party has clearly marked such Party Data as 'confidential', subject to the exemptions set out in SEC Section M4.11;
3. Information related to threat assessments, security incidents and vulnerabilities with the potential to affect smart metering security will be treated as 'confidential' to facilitate key industry and other security experts in proactively managing security risks, amending security requirements and overseeing security assurance on an ongoing basis;
4. The Panel, its Sub-Committees, Working Groups - including when acting via SECAS or SECCo - will operate a policy of non-disclosure to protect Party Data, and will only discuss that Party Data at Panel or Sub-Committee meetings or Working Groups, where non-confidential information is shared by members of the governance groups, members should ensure the information is accompanied by appropriate context;
5. Party Data will not be disclosed as part of any publicly available information distributed or published by SECAS on behalf of the Panel, SECCo, Sub-Committees, or Working Groups, and will only be circulated to the aforementioned organisations on a strictly need to know basis; and
6. The lowest possible appropriate classification should be applied to encourage transparency across the governance groups, SEC Parties, and wider SMIP stakeholders, for the purpose of visibility of key decisions and their rationale. The default classification will be Green, including for all DCC programme artefacts, and clear justification will be provided for any more restricted classification. Downgrading of documents after key decisions have been made at a governance group meeting should take place wherever possible and be carried out by the document author or with their written approval.

## 5. Governing the Panel Information Policy

### 5.1 SEC Party responsibilities

SEC Parties are responsible for notifying and marking documents or any media that contain sensitive information which need to be protected when being handled by the Panel, its Sub-Committees, Working Groups, SECAS and SECCo (M4.8 (a)). To ensure the protection is handled in line with industry good practice, any documentation or media provided to SECAS should have clear labelling applied. Appendix B provides some recommendations for application of classification labelling, but SEC Parties may mark documentation or media as they see fit. The DCC is subject to separate labelling obligations under SEC Section M4 (Confidentiality) and defines its own classifications in its own DCC Information Classification and Handling document (as summarised in Appendix A).

Please note that this document does not supersede or replace any of the applicable provisions defined within the Code or elsewhere and that other data protection measures, such as the Data Protection Act 2018, still apply to all Data (including Party Data).

## **5.2 SEC Panel and Sub-Committee responsibilities**

Members of the Panel, along with its Sub-Committees, Working Groups, including SECCo and SECAS shall all ensure they understand and act in accordance with this policy and the principles of non-disclosure and other relevant Code obligations when managing Party Data

Where the Panel, along with its Sub-Committees, Working Groups, and including SECCo and SECAS, are in receipt of Data which is unmarked, yet believe the content may be classified, SECAS shall contact the submitting Party to enquire as to whether the Data should in fact be marked as confidential (or, where provided by the DCC, 'controlled' or 'confidential').

The Panel is responsible for the governance of this Policy and any amendments to it will require its approval. The approved document should be shared and communicated with the relevant parties covered by this Policy.

This Policy will be reviewed at annually intervals, as determined by the Panel, or if significant changes occur, to ensure its continuing suitability and effectiveness.

## **5.3 SECAS responsibilities**

SECAS, on behalf of the Panel, is responsible for the day-to-day administration of this Policy, and Party Data received and disseminated on behalf of the Panel, Sub-Committees, Working Groups and SECCo.

Where the Panel, along with its Sub-Committees, Working Groups, and including SECCo and SECAS, are in receipt of Data which is unmarked, yet they believe the content may be classified, SECAS shall contact the submitting Party to enquire as to whether the Data should in fact be marked as confidential. If the DCC provides unmarked data, SECAS will request a new version to be marked with one of the four DCC classifications (DCC 'public', 'controlled', 'controlled – SEC Parties', 'confidential'), before using or sharing the data.

## **6. Handling, labelling, and storing confidential Data**

SEC Section M4.8 defines the classifications available to SEC Parties. All Party Data received should be classified at source and handled accordingly. It is the responsibility of the SEC Party, and any organisation or body sharing SEC Party data to do so. This section describes the classifications available to SEC Parties and the associated processes for labelling, handling and storage of information in accordance with its classification.

Appendix B contains the SEC Panel Information Classification and Handling Matrix for more comprehensive guidance of handling, labelling, and storing confidential Data.

### **6.1 Confidential data**

Confidential data includes Security, commercially sensitive information and Personal Data.

SEC Section M4.8 states that where a SEC Party wishes its Party Data to remain confidential it shall clearly mark such Party Data as 'confidential'. SEC Section M4.10 states that the Panel shall not

disclose, or authorise access to, any Party Data provided to it by a Party where that Party has clearly marked such Party Data as confidential (or, where provided by the DCC as 'controlled' or 'confidential'). Confidential data falls under the SEC paper classification RED (see Appendix B).

SEC Section M4.11 describes the circumstances where the duty of confidentiality does not apply:

- where the Panel is compelled to disclose in accordance with Laws and Directives<sup>1</sup> or instructions of the Authority;
- where such Party Data is already available in the public domain<sup>2</sup>; and/or
- where such Party Data is already lawfully in the possession of the Panel other than as a result of the Code and/or the DCC Licence.

## 6.2 Labelling

Anyone wishing to provide confidential Party Data to the Panel, its Sub-Committees and Working Groups, SECAS and/or SECCo, should make sure that the relevant classification labelling is clearly applied. Recommendations and guidelines for appropriate labelling is provided in Appendix B and applies to media in all formats.

## 6.3 Handling

Where a SEC Party has marked its Party Data as confidential (or, where provided by the DCC, 'confidential' or 'controlled'), the following handling rules shall apply to the Panel (and its Sub-Committees and Working Groups, SECCo and SECAS):

- the exchange of Data between the Panel, its Sub-Committees and Working Groups, SECAS and/or SECCo, authorised users, external companies or agencies shall be carried out in a responsible and secure manner using secure protocols (Egress Switch Platform or Microsoft Teams<sup>3</sup>) when moving information outside of the internal LAN infrastructure (provided by SECAS) or secure file repositories
- SECAS shall ensure electronic methods of transfer identified provide for the necessary level of protection, commensurate with the classification of the Data; and
- the transfer Data from SECAS shall always be accomplished using secure protocols (Egress Switch Platform or Microsoft Teams) when moving information outside of the internal LAN infrastructure (provided by SECAS) or secure file repositories.

Regarding the release of Data by SECAS as referred to in the final bullet point above, this shall only be permitted where:

- such disclosure is permitted in accordance with the Code and/or the Authority to do so has been explicitly received from the relevant SEC Party for the Data; and
- routing or transfer is to a named and authorised individual (no generic email accounts are permitted) in order to support audit activities.

---

<sup>1</sup> Means any law (including the common law), statute, statutory instrument, regulation, instruction, direction, rule, condition or requirement (in each case) of any Competent Authority (or of any authorisation, licence, consent, permit or approval of any Competent Authority).

<sup>2</sup> Other than as a result of a breach by the Panel.

<sup>3</sup> See Section 6.7 for more information.



To facilitate the appropriate handling of Party Data by the Panel (and its Sub-Committees and Working Groups, SECCo and SECAS), the colour-coded classification and handling rules set out in Appendix B shall be used.

## 6.4 Storage

Data shall be stored in as few places as possible and archived or destroyed when no longer required in line with Code requirements. The following principles shall also apply to the storage of Party Data:

- Party Data that has the potential to be stored on a long-term basis shall be kept in a secure location with limited access. Other forms of information, including meeting recordings and transcripts, will be stored on a short-term basis in line with agreed guidance;
- Any confidential Party Data that is distributed to Panel Members, Sub-Committee Members or Working Group members, must be done so via a link to the secure paper platforms or as an attachment to a secure, encrypted email. Any confidential Party Data must not be stored or retained in any format by Panel Members, Sub-Committee Members or Working Group members for any longer than 5 Working Days (WD) of receipt, or following the relevant committee meeting; and
- Panel Members / Sub-Committee Members / Working Group members / SECAS employees should always be conscious of their surroundings when engaged in confidential conversations (i.e. verbal exchange of confidential information via telephone, video conference, WebEx etc.) or when reviewing / displaying information on their laptop outside of their office environment.

## 6.5 Retention

When information is no longer required for the purposes of the Code, it shall be retained in line with legal requirements or destroyed in a manner commensurate with the classification and sensitivity of the Data to ensure there is no possibility of compromise.

Data retention principles:

- where there is the need to retain confidential Party Data, the submitting SEC Party shall be consulted on the Data retention period
- for Data where the SEC Panel is acting as a Joint Data Controller, as defined by the ICO guidelines<sup>4</sup>, they shall agree a Data retention period in collaboration with all participating organisations acting in a similar capacity
- where it is not possible to clearly define a Data retention period, there shall be an annual review date defined in the information asset register or Record of Processing Activities which will ensure a review of the retention requirements and indicate the document author to carry out the review
- retention conditions shall be designed to protect records against unauthorised access, loss, falsification, destruction and theft; and

---

<sup>4</sup> <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

- storage systems and solutions used for the retention of electronic records shall be designed in such a way that the archived records remain accessible, authentic, reliable and usable during their retention period.

Further details on the Data retention principles are set out in the [SECCo Data Retention Policy](#).

## 6.6 Confidentiality and Disclosure Agreement

All members and Alternates of the Panel, its Sub-Committees and Working Groups will be requested to sign a confidentiality and disclosure agreement prior to them being able to attend any meetings or receive any documentation. This shall also apply to any administrative or executive assistants working on behalf of, and as nominated by, all members and Alternates of the Panel, its Sub-Committees and Working Groups, who are in receipt of Panel information in any capacity and in any format or medium. The agreement states that they have understood the relevant Terms of Reference, all of which will include the classification table and state that they understand the information sharing levels confidentiality and disclosure obligations.

## 6.7 Secure paper platforms

Given the confidential nature of some of the documentation distributed on behalf of the Panel, SECAS identified the need for a secure distribution platform.

### Egress Switch Platform

Egress Switch was identified as an appropriate tool (following a risk assessment process and review by the SSC) for the dissemination of classified information, following a risk assessment against all information assets described in SEC Sections G, I and L.<sup>5</sup> The Egress Switch secure workspace has the following security features and classifications<sup>6</sup>:

- secures data at rest and in transit using AES-256-bit encryption
- utilises FIPS 140-2 certified libraries
- secure authentication and user enrolment
- ISO 27001:2013 certified
- Cyber Essentials Plus certified
- Skyhigh Cloud Trust™ rating of Enterprise-Ready
- Uses data centres accredited to ISO 27001/9001; and
- Listed under Cyber Security Supplier to Government Scheme.
  - Legacy UK Gov scheme (ended March 2022)  
<https://www.gov.uk/government/publications/cyber-security-supplier-to-government-scheme/cyber-security-supplier-to-government-scheme-guidance-for-applicants#:~:text=This%20scheme%20will%20run%20until%20March%202022>.

<sup>5</sup> More information on the platform is available here <https://www.egress.com/products/file-sharing-and-collaboration-suite/workspace>

<sup>6</sup> [https://www.egress.com/media/o15j450r/egress\\_secure\\_workspace\\_datasheet\\_us.pdf](https://www.egress.com/media/o15j450r/egress_secure_workspace_datasheet_us.pdf)

Following a request from the SSC, and approval by the SECCo Board in February 2019, all participants, including administrators, must use multi-factor authentication when using Egress.

### Microsoft Teams

In order to improve ease of access and collaboration on papers, SECAS rolled out the use of MS Teams in 2021. MS Teams is now used as the principal platform for sharing all Panel, Sub-Committee, and Working Group documentation besides that of the Security Sub-Committee (SSC) and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA). Egress remains in use for SSC/ SMKI PMA papers, as well as any matters deemed confidential, such as Privacy Assessments. Access to MS Teams is only granted to Panel, Sub-Committee, and Working Group members who have signed an NDA, and relevant SECAS staff. SECAS regularly audits permissions following changes in membership.

Teams enforces team-wide and organisation-wide two-factor authentication, single sign-on through Active Directory, and encryption of data in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption.<sup>7</sup> As with Egress, MS Teams secures data at rest and in transit using AES-256-bit encryption and utilises FIPS 140-2 certified libraries.<sup>8</sup>

## 6.8 Downgrading papers

According to the Principles of the Panel Information Policy, downgrading of documents after key decisions have been made at a governance group meeting should take place wherever possible.

In practice, SECAS should follow the following process:

- Obtain written consent to downgrade an existing document by the document author and the governance group Chair
- OR obtain a downgraded (e.g. redacted) version of the document from the author, with permission from the governance group Chair
- Upload a PDF version of the downgraded document to the SEC website (if Clear or Green) with relevant permissions applied
- Embed a link to the document to the web page for the relevant meeting, as a stand-alone file (i.e. not in a zip file) to ensure an audit trail; and
- Notify the intended new audience (i.e. SEC Parties) via email, sharing a link to the web page.

If a document has been downgraded following a governance group meeting (e.g. Amber to Green), and the Chair agrees the associated discussion is also of the same classification as the downgraded paper (e.g. Green) the associated minutes may also be downgraded (e.g. included in the Green set of minutes).

If a paper is downgraded from Red to Amber, SECAS should not share via the SEC website but should instead upload the Amber version to the governance group MS Teams site, and notify members of its availability, should they wish to share it.

---

<sup>7</sup> <https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide>

<sup>8</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption>

## Appendix A DCC Classifications

This Appendix describes the classifications available to the DCC, as per the Code, and the associated provisions, including the DCC's Information Classification and Handling Standard. As this covers the DCC providing information to SEC Parties, this section does not include handling, storage or retention policies.

### 1. Classifications

#### 1.1 DCC Confidential

When providing Data for the purposes of SEC Section M4.8 (Confidentiality and the Panel) and SEC Section M4.15 (Confidentiality of the DCC), the DCC may only mark such Data as confidential where:

- (a) that Data relates to a DCC Service Provider providing services pursuant to a DCC Service Provider Contract which was referred to in paragraph 1.5 of schedule 1 to the DCC Licence on its grant
- (b) the DCC is subject to an existing obligation under the DCC Service Provider Contract referred to in paragraph (a) to ensure that that Data remains confidential
- (c) the DCC's Liability for breaching the obligation referred to in paragraph (b) is unlimited; and
- (d) the DCC is not prohibited from marking that Data as 'confidential' under SEC Section M4.24 (see paragraph 1.5 below).

DCC Confidential Information is the highest level of classification and is equal to SEC Red classification. According to the DCC's Information Classification and Handling Standard, DCC confidential Information must only be disclosed to named individuals to whom permission has been given for it to be disclosed, and/or to those with a 'Need To Know', who are cleared to receive the information and are verified as having necessary confidentiality obligations in place with DCC.

#### SEC Alternative

DCC Confidential is equal to the SEC Red classification in terms of how this Data is handled, shared, and stored by SECAS, the Panel and its Sub-Committees (see Appendix B for further guidance).

#### Confidential Liability

Each SEC Party's Liability for breaches of Data marked as confidential shall be unlimited in accordance with SEC Section C2.3.

#### 1.2 DCC Controlled

For the purposes of SEC Section M4.8 (Confidentiality and the Panel) and SEC Section M4.15 (Confidentiality of DCC data), the DCC may only mark such Data or Party Data as controlled where:

- The uncontrolled disclosure of, or uncontrolled authorised access to, that Data could reasonably be considered to be prejudicial to the DCC (or any DCC Service Provider); and The DCC is not prohibited from marking that Data as 'controlled' under SEC Section M4.24 (see paragraph 1.5 below).

According to the DCC's Information Classification and Handling Standard, DCC Controlled signals that the information is sensitive to Smart DCC and/or its suppliers but is not suitable for the public

domain. DCC Controlled information can be disclosed to individuals and groups in Smart DCC, and third party individuals and groups who:

- need to see it in order to provide to, or receive goods or services from, DCC; and
- are verified as having necessary confidentiality obligations (e.g. Contractual Terms, Non-Disclosure Agreement (NDA) or SEC or REC obligations) in place with DCC.

Permission to share DCC Controlled information externally must come from the information owner and must be captured in writing.

### **SEC Alternative**

DCC controlled is equal to the SEC Amber classifications in terms of how this Data is handled, shared, and stored by SECAS, the Panel and its Sub-Committees (see Appendix B for further guidance).

### **Controlled Liability**

Each SEC Party's Liability for breaches of Data marked as controlled shall be limited to £1,000,000 in accordance with SEC Section M2.3.

## **1.3 DCC Controlled – SEC Parties**

This sub-category of DCC Controlled is used where SEC Parties may access documentation and was created to align with the SEC alternative classification 'Green'. This classification would be used for handling documentation shared with no confidential information, for example technical presentations to SEC Panel and SEC Sub-Committees, therefore allowing information to be shared with the Parties they represent on a controlled need to know basis.

### **SEC Alternative**

DCC Controlled (SEC Parties) is equal to the SEC Green classifications in terms of how this Data is handled, shared, and stored by SECAS, the Panel and its Sub-Committees. This means DCC Controlled (SEC Parties) Data is made available to SEC Parties, as per the Green SEC classification (see Appendix B for further guidance).

SECAS will assume any papers marked DCC Controlled are to be treated as AMBER-STRICT, unless specifically titled DCC Controlled (SEC Parties) or DCC confirms in writing otherwise.

## **1.4 DCC Public**

DCC Public signals that information is non-sensitive and may be placed in the public domain.

DCC Public is also applied to information that the DCC Licence requires the DCC to publish. DCC Public must be applied to information such as press releases, public blogs, 'industry insights', job advertisements and client brochures which are placed in the public domain.

Non-sensitive business information such as public industry forum presentations, guidance notes and ordering policies must be classified as DCC Public to signal that it does not hold any sensitive information which needs to be protected. Marking this information as DCC Public does not mean that it must be placed in the public domain, but it must be classified DCC Public to reflect its sensitivity.

### **SEC Alternative**

DCC Public is equal to the SEC Clear classifications in terms of how this Data is handled, shared, and stored by SECAS, the Panel and its Sub-Committees (see Appendix B for further guidance).

## 1.5 Unmarked

Where the DCC provides Data not marked as 'confidential' or 'controlled' or 'public', SECAS shall contact the DCC to request that a classification is applied.

## 1.6 Restrictions

SEC Section M4.24 states that the DCC shall not mark data as either 'confidential' or 'controlled' where or to the extent that:

- the DCC is expressly required to place that Data in the public domain in order to comply with its duties under Laws and Directives
- it is necessary for the exercise by the DCC of any of its obligations under the Electricity Act, the Gas Act, the DCC Licence, or this Code to place that Data in the public domain; or
- that Data is already in the public domain other than as a result of a breach by the SEC Parties or the Panel of SEC Section M4 and/or the DCC Licence.

## 2. Distribution and Receipt of DCC Data

SEC Section M4.20 states that no SEC Party other than DCC shall disclose, or authorise access to, Data that is marked as either 'confidential' or 'controlled'<sup>9</sup>. Therefore, if a SEC Party wishes to receive confidential or controlled DCC Data they should do so in accordance with the provisions below.

### 2.1 Receiving Confidential DCC Data

Where a SEC Party wishes to receive Data which the DCC has classified as 'confidential', the SEC Party shall provide the DCC with a list of names and contact details of individuals who are authorised by it to receive such Data. The 'CC shall only' issue 'confidential' Data to those named individuals within the SEC Party and it shall not be provided to the SEC Party as a whole.

Where no listing of individuals has been provided to the DCC the DCC are under no obligation to disclose any 'confidential' Data to that SEC Party. Any 'confidential' DCC Data received by a SEC Party shall not be disclosed by that SEC Party. These restrictions on disclosure and access shall not apply to the extent that:

- the SEC Party disclosing the Data does so in accordance with duties under Laws and Directives or instructions of the Authority
- the Data is already available in the public domain
- the Data is already lawfully in the possession of the SEC Party via a means other than the result of the Code or the DCC Licence; or
- the Data is marked as confidential, but the DCC has disclosed it to the SEC Party by providing it to an individual not nominated by the SEC Party as an individual authorised to receive confidential Data, and the SEC Party has complied with the requirements of SEC Section M4.20(d).

---

<sup>9</sup> Subject to exemptions stated in SEC Section M4.20

In general, requests for access to Confidential Data should be made via [servicedesk@smartdcc.co.uk](mailto:servicedesk@smartdcc.co.uk).

## **2.2 Receiving Controlled DCC Data**

There are no prerequisites in order for SEC Parties to receive DCC Controlled Data.

Any 'controlled' DCC Data received by a SEC Party shall not be disclosed by that SEC Party. These restrictions on disclosure and access shall not apply to the extent that:

- the SEC Party disclosing the Data does so in accordance with duties under Laws and Directives or instructions of the Authority;
- the Data is already available in the public domain; or
- the Data is already lawfully in the possession of the SEC Party via a means other than the result of the Code or the DCC Licence.

SEC Parties may receive Data marked DCC Controlled (SEC Parties), where applicable.

## Appendix B: SEC Governance Classifications

This appendix describes the classifications available to the Panel, its Sub-Committees and Working Groups, SECCo, SECAS and all SEC Parties. All documentation issued by one of these bodies will be marked in accordance with this document.

These classifications only apply to Data issued by and shared between the Panel, its Sub-Committees and Working Groups, SECCo and SECAS

SEC Parties wishing to provide Data to any of these bodies should use the classifications described in Section 6.1 of the body of this Policy, as defined in SEC Section M4.

All Data issued from the Panel, its Sub-Committees, Working Groups, SECAS and SECCo shall be assigned a classification in accordance with the table below.

SEC Parties should familiarise themselves with the table below and be cognisant of the restrictions in place at each classification level.

| Classification | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RED</b>     | <p>For the eyes and ears of individual members of the governance group only, no further disclosure. RED information must not be shared with anyone else; information is limited to those individual members of the governance group including alternates (Panel/ Sub-Committee/ Working Group) and direct recipients of the material. All recipients must have signed an NDA stating their acceptance to abide by these terms.</p> <p>Agenda items marked as RED will be discussed in a closed, confidential session and discussions will only be included in minutes marked as RED.</p> | <p>RED Data indicates significant risk for the security, privacy, reputation or operation of organisations involved.</p> <p>Common examples of RED-classified information can be found in Appendix C. RED is the equivalent to DCC Confidential, as defined by Section M4.22 of the SEC. Any DCC Confidential documents which are circulated to the Panel, its Sub-Committees or Working Groups, will be treated the same as a RED SECAS document.</p> <p>RED-classified information is to be shared with members of the specific governance group via the Egress Switch Platform if containing Security or Privacy content or if specifically requested by the information owner. Microsoft Teams will be the principal platform for distributing all other content in accordance with Section 6.7.</p> |



| Classification           | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | Any documentation classified as RED shall be distributed using the agreed secure storage and distribution platforms.                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>All RED documents should be shared in a non-editable format (e.g. PDF) unless the author requires direct input into the development of the document.</p> <p>RED material can also be shared with SECCo employees representing SECCo. The documentation should clearly specify SECCo employees as the audience. This excludes Security or Privacy content.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>AMBER-<br/>STRICT</b> | <p>Limited disclosure, recipients can only distribute this on a strict need-to-know basis within their SEC Party Category to protect and prevent harm.</p> <p>This information can be restricted to a specified, narrower audience in some cases which should be clearly articulated on the document. An example would be anonymised details of a security incident or vulnerability that needs to be communicated on a strict need-to-know basis to enable appropriately qualified security specialists to implement prevention or mitigation actions.</p> | <p>Examples of AMBER-STRICT classified information can be found in Appendix C.</p> <p>AMBER-STRICT is the equivalent to DCC Controlled, as defined by Section M4.23 of the SEC.</p> <p>Any DCC Controlled documents which are circulated to the Panel, its Sub-Committees or Working Groups must be marked as AMBER-STRICT if the desired audience is limited to sharing within the SEC Party category and not with third party stakeholders who are not SEC Parties.</p> <p>Microsoft Teams will be the principal platform for distributing all AMBER-STRICT information in accordance with Section 6.7 unless a narrower audience has been determined, in which case Egress Switch platform will be used.</p> <p>All AMBER-STRICT documents should be shared in a non-editable format (e.g. PDF) unless the author requires direct input into the development of the document.</p> |

| Classification | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AMBER</b>   | <p>Limited disclosure, recipients can only distribute this within their SEC Party Category and third party stakeholders (who have a contractual relationship with that SEC Party) including Trade Associations on a need-to-know basis to protect and prevent harm.</p> <p>Agenda items marked as AMBER or AMBER-STRICT will be discussed in a closed, confidential session and discussions will only be included in the Confidential minutes marked as AMBER.</p> <p>Examples of third party stakeholders include Trade Associations and contracted organisations within the supply chain (such as service providers, vendors, or a third party which has a contractual relationship with a SEC Party).</p> | <p>AMBER applies when information requires support to be effectively acted upon, yet carries risk to security, privacy, reputation, or operations if shared outside of the organisations involved. It can be broadly categorised as information which is restricted to a certain governance group. AMBER documents can be shared beyond the target governance group to those who have a need to know in order to take action and can only be shared by members within their SEC Party Category and third party stakeholders such as Trade Associations.</p> <p>Common examples of AMBER-classified information can be found in Appendix C.</p> <p>AMBER-classified information may be shared with members of the specific governance group via the Egress Switch Platform or as an attachment to a secure, encrypted email.</p> <p>Microsoft Teams will be the principal platform for distributing all AMBER information.</p> <p>All AMBER documents should be shared in a non-editable format (e.g. PDF) unless the author requires direct input into the development of the document.</p> |
| <b>GREEN</b>   | <p>Limited disclosure, recipients can distribute this information to SEC Parties and SMIP stakeholders but not made publicly available.</p> <p>GREEN will be the default classification for any discussions unless otherwise notified.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>GREEN applies when information is useful to increase awareness with SEC Parties. GREEN Data is information which should be shared for the benefit of SEC Parties but cannot be made completely public.</p> <p>Common examples of GREEN-classified information can be found in Appendix C.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Classification | Definition                                                                                                                                                                                                                                                                 | Criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <p>In practice, GREEN documentation is stored on the SEC website with password restrictions so SEC Parties can only access the documents after logging in.</p> <p>Agenda items marked as GREEN will be included in the minutes marked as GREEN.</p>                        | <p>GREEN is the equivalent to DCC Controlled (SEC Parties). Any DCC Controlled (SEC Parties), documents which are circulated to the Panel, it's Sub-Committees or Working Groups, will be treated the same as a GREEN SECAS document.</p> <p>Green classified information may be shared with SEC Parties via the SEC website restricted to SEC Parties.</p> <p>All GREEN documents should be shared in a non-editable format (e.g. PDF) unless the author requires direct input into the development of the document.</p> |
| <b>CLEAR</b>   | <p>Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.</p> <p>Agenda items marked as CLEAR will be included in the Non-confidential minutes marked as CLEAR.</p> | <p>Sources may use CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p> <p>Common examples of CLEAR-classified information can be found in Appendix C.</p> <p>CLEAR is the equivalent to DCC Public. Any DCC Public documents which are circulated to the Panel, it's Sub-Committees or Working Groups, will be treated the same as a CLEAR SECAS document.</p>                                                            |

**Table 1: Classification Table**

## Appendix C: Artefacts Matrix

This appendix describes the classifications applied to standard SEC artefacts.

| Classification | Common artefacts with this classification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RED</b>     | <p>The following are common examples of RED-classified information:</p> <ol style="list-style-type: none"> <li><b>1. Party Data:</b></li> <li>Events of Default (SEC Section M8.1), including SEC Section G9.34 for Security Breach Events of Default.</li> <li>The decision and all other information pertaining to a Party arbitration (M7.6(g))</li> <li>Financial Information (for example debt, Credit Cover).</li> <li>Non-compliant Parties, Privacy Assessment papers and supporting evidence</li> <li><b>6. Commercially sensitive data.</b> This includes named commercial entities, for example in relation to procurements, as well as DCC cost information.</li> <li><b>7. Security and Privacy data:</b> <ul style="list-style-type: none"> <li>Findings of Security or Privacy Assessments.</li> <li>Evidence submitted as part of Security or Privacy Assessments</li> <li>Security or vulnerability reports identifying a Party.</li> <li>Detailed Threat and Risk Assessments that identify a Party or a Device Manufacturer or an identified vulnerability.</li> <li>Specific details of security breaches.</li> <li>Specific security advice to the DCC that cannot be shared beyond the DCC Security Team.</li> <li>'Sensitive' personal data i.e. criminal convictions data or 'special categories of personal data' under the Data Protection Act 2018.</li> </ul> </li> <li><b>8. DCC's Post-Commissioning reports</b></li> <li><b>9. SECCo Board Risk and Issues Register</b></li> <li><b>10. Panel and Sub-Committee Risk and Issues Registers (if featuring a risk or issue classified as RED)</b></li> <li><b>11. DCC Programme Business Cases</b></li> <li><b>12. Privacy Change Notification Requests</b></li> <li><b>13. Confidential consultation responses</b></li> <li><b>14. Confidential Actions</b>, whereby all Actions are RED-classified.</li> <li><b>15. Confidential Agendas</b>, such as SSC agendas</li> </ol> |

| Classification      | Common artefacts with this classification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <b>16. Confidential post-meeting documentation and media in any format or medium, where agenda items were RED-classified</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>AMBER-STRICT</b> | <p>The following are common examples of AMBER-STRICT-classified information:</p> <ol style="list-style-type: none"> <li><b>1. Security and Privacy Data:</b> <ul style="list-style-type: none"> <li>• Security Architecture document with sequence diagrams.</li> <li>• Risk assessments identifying specific threat actors.</li> <li>• Specific security advice to the DCC that needs to be shared with a specific Service Provider.</li> <li>• Personal data ie. Energy Consumer names, addresses, MPxNs (other than business contact details)</li> </ul> </li> <li><b>2. SECCo Board documentation</b></li> <li><b>3. Work Packages and Lookback Reports</b></li> <li><b>4. Supplier contracts</b></li> <li><b>5. Programme readiness updates</b></li> <li><b>6. Major Incident reports</b></li> <li><b>7. Panel and Sub-Committee Risk and Issues Registers (if featuring a risk or issue classified as AMBER-STRICT)</b></li> <li><b>8. Sensitive Alt-HAN information</b></li> <li><b>9. DCC Testing Completions</b> (SREPT, UEPT, SMETS1 Eligibility Testing) and DCC Testing Notifications</li> <li><b>10. Applicants going through the Accession process</b> (until the SECCo Board approves the Accessions)</li> <li><b>11. Confidential Agendas</b>, such as SSC agendas</li> <li><b>12. Confidential Actions</b>, whereby all Actions are AMBER-STRICT classified</li> </ol> <p><b>13. Confidential post-meeting documentation and media in any format or medium, where discussions are classified as AMBER-STRICT</b></p> <p><b>14. Some draft documents</b>, such as unapproved Project Briefs, Project Budgets, or draft correspondence or consultation responses</p> |
| <b>AMBER</b>        | <p>The following are common examples of AMBER-classified information:</p> <ol style="list-style-type: none"> <li><b>1. Security and Privacy data:</b> <ul style="list-style-type: none"> <li>• General, anonymised advice about lessons learned on security incidents and vulnerabilities.</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Classification | Common artefacts with this classification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <ul style="list-style-type: none"> <li>• General advice on security threats and risks.</li> <li>• General security advice to the DCC that can be shared across Service Providers.</li> </ul> <ol style="list-style-type: none"> <li>2. <b>Panel and Sub-Committee Risk and Issues Registers (if featuring a risk or issue classified as AMBER)</b></li> <li>3. <b>DCC operational updates, including installation and migration data</b></li> <li>4. <b>Confidential Actions</b>, whereby all Actions are AMBER-classified</li> <li>5. <b>Confidential post-meeting documentation and media in any format or medium, where agenda items were AMBER-classified</b></li> </ol>                                                                                              |
| <b>GREEN</b>   | <p>The following are common examples of GREEN-classified information:</p> <ol style="list-style-type: none"> <li>1. <b>SEC Panel Transitional Governance reports</b></li> <li>2. <b>Problem Statements</b></li> <li>3. <b>Project Briefs</b></li> <li>4. <b>Project Definition Documents (PDDs)</b></li> <li>5. <b>Project Initiation Documents (PIDs)</b></li> <li>6. <b>Some draft consultation responses</b></li> <li>7. <b>Non-confidential Actions Logs</b>, where all actions are GREEN-classified</li> <li>8. <b>Non-confidential post-meeting documentation and media in any format or medium, where all agenda items were GREEN-classified</b></li> <li>9. <b>Information relating to unpublished podcasts</b></li> <li>10. <b>Template contracts</b></li> </ol> |

| Classification | Common artefacts with this classification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CLEAR</b>   | <p>The following are common examples of CLEAR-classified information:</p> <ol style="list-style-type: none"> <li>1. <b>Administrative SECAS paper</b>, such as elections information and meeting dates</li> <li>2. <b>SECAS reporting</b>, such as the Sub-Committee report</li> <li>3. <b>Public-facing resources</b>, such as newsletters, privacy policies, staff contact details listed on the SEC website</li> <li>4. <b>Non-confidential agendas</b></li> <li>5. <b>Non-confidential Actions Logs</b>, where all actions are CLEAR-classified</li> <li>6. <b>Non-confidential post-meeting documentation and media in any format or medium</b>, where all agenda items were CLEAR-classified</li> <li>7. <b>SEC Modification Reports</b></li> <li>8. <b>SEC Modification Timetable paper</b></li> <li>9. <b>SEC Releases Update paper</b></li> <li>10. <b>SEC Change Report</b></li> <li>11. <b>SEC Modification Progression paper</b></li> <li>12. <b>Change Board votes</b></li> <li>13. <b>Non-confidential consultation responses</b></li> </ol> |

**Table 1: Classification Table**