This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to

Paper Reference:	**SECP_78_1303_08**
Action:	**For Decision**

Panel Information Policy Update

1. Purpose

The Panel Information Policy is a document that the Panel has established to maintain, classify, handle, and store Party Data in accordance with SEC Section M4.13 and M4.14.

Appendix A to this paper sets out amendments to the Panel Information Policy to clarify the exceptions that apply to the Authority's access to confidential information and to state that the Secretary of State and the Authority are not required to sign Non-Disclosure Agreements (NDAs) in order to participate at SEC Panel, Sub-Committee or Working Group meetings.

The Panel is requested to approve the amendments to the Panel Information Policy.

2. Panel Information Policy Amendments

A track changed version of the policy is provided in Appendix A to this paper which outlines amendments to:

- Section 3 (Principles): amendments have been made to the wording to clarify the principles of the Panel Information Policy.
- Section 7.4 (Handling): additional wording has been added to permit the release of Data by SECAS when required under Laws and Directives or requested by the Authority.
- Section 1.1 (Appendix B): additional wording has been added to exempt the Authority and representatives of the Secretary of State from signing confidentiality and disclosure agreements prior to attending SEC Panel, Sub-Committee or Working Group meetings.

3. Recommendations

The SEC Panel is requested to **APPROVE** version 4.1 of the Panel Information Policy.

Louise Evans;

SECAS Team; 6 March 2020

Attachments: Appendix A: Panel Information Policy v4.1

SEC
Smart Energy Code

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to

Smart Energy Code

Panel Information Policy

Version 4.1

13 March 2020

Change History

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
4.1	Draft	13/03/2020	SECAS	Amended wording for sharing of information with the Authority

Document Controls

REVIEWER	ROLE	RESPONSIBILITY	DATE
SEC Panel	Document Approver	Panel Information Policy Owner	20th May 2016
SEC Panel	Document Approver	Panel Information Policy Owner	11th November 2016
SEC Panel	Document Approver	Panel Information Policy Owner	15th March 2019

Date of next review: 10/02/2021~~0~~

Contents

1. Purpose 5
2. Party Data 5
3. Principles 5
4. Scope 6
5. Application of the Panel Information Policy 6
6. Responsibility for Compliance 7
6.1 Roles and Responsibilities 7
6.2 Controls 7
6.3 Unmarked Documents and SECAS Assistance 7
7. SEC Classifications 7
7.1 Confidential 7
7.2 Unmarked 8
7.3 Labelling 8
7.4 Handling 8
7.5 Storage 9
7.6 Retention 9
Appendix A: DCC Classifications
1. Classifications 11
1.1 Confidential 11
1.1.1 Confidential Liability 11
1.2 Controlled 11
1.2.1 Controlled Liability 11
1.3 Public 11
1.4 Unmarked 12
1.5 Restrictions 12
1.6 Distribution and Receipt of DCC Data 12
1.6.1 Receiving Confidential DCC Data 12
1.6.2 Receiving Controlled DCC Data 13
APPENDIX B: SEC Governance Classification Rules
1. Panel, Sub-Committees and Working Groups, SECAS and SECCo 14
1.1 Confidentiality and Disclosure Agreement 15
1.2 Egress 15
Annex A : SEC Panel Information Classification and Handling Matrix 16
Annex B: Retention and Destruction of Data by the Panel 18

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 it is, henceforth 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 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.

The scope of this document has been expanded to include other information which may be of use to SEC Parties. Appendix B of this document explains the classifications available to the Panel, its Sub-Committees, Working Groups, SECCo and the Smart Energy Code Administrator and Secretariat (SECAS). Appendix B also explains the distribution rules associated with each classification level, as well as how agenda items at each classification level will be recorded. Appendix A of this document explains the classifications available to the DCC; SEC Parties should refer to this section if they are in receipt of classified DCC information.

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

2. Party 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 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, reports, forecasts, images or sounds (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.

3. Principles

This Panel Information Policy is underpinned by the following principles:

- Party Data will only be requested by the Panel, its Sub-Committees, Working Groups, the Authority - 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), The Electricity Act 1989 and The Gas Act 1986;

- 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;
- 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; and
- 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.

4. Scope

SEC Section M4.13 states that the Panel must establish a policy 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 Section G (Security), Section I (Data Privacy), and Section L (Smart Metering Key Infrastructure) and its related SEC Subsidiary Documents. This includes but is not limited to, Party Data received in relation to User Security Assessments, Other User Privacy Audits and compliance assessments of Smart Meter Key Infrastructure (SMKI) Participants. 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).

Appendix B of this document describes the classifications which the Panel (and its Sub-Committees and Working Groups, SECAS and SECCo) have available to them and provides descriptions of each level. Appendix B provides a description of the classifications available to the DCC when they are providing information in relation to Code activities and they wish for the provisions and measures of SEC Section M2 to apply. Finally, Annex A provides some guidelines and recommendations for application of classified labelling for those who wish to provide classified data to the Panel (and its Sub-Committees and Working Groups, SECAS and SECCo).

5. Application of the Panel Information Policy

SEC Parties are responsible for notifying and marking documents that contain sensitive information that needs to be protected when being handled by the Panel along with its Sub-Committees, Working Groups, SECAS and SECCo. To ensure the protection is handled in line with industry good practice, any documentation provided to SECAS should have clear labelling applied. Annex A provides some recommendations for application of classification labelling but SEC Parties may mark documentation as they see fit. The DCC is subject to separate labelling obligations under SEC Section M4 (Confidentiality).

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, still apply to all Data (including Party Data).

6. Responsibility for Compliance

6.1 Roles and 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.

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.

SECAS 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.

6.2 Controls

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

6.3 Unmarked Documents and SECAS Assistance

Where the Panel, along with its Sub-Committees, Working Groups, 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 (or, where provided by the DCC, 'controlled' or 'confidential').

7. SEC Classifications

SEC Section M4.8 defines the classifications available to SEC Parties. All Party Data received should be classified at source and it is the responsibility of the SEC Party 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.

7.1 Confidential

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, 'controlled' or 'confidential').

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[1] or instructions of the Authority;

[1] 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).

- where such Party Data is already available in the public domain[2]; 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.

7.2 Unmarked

Without prejudice to section 6.3 of this policy, in accordance with SEC Section M4.9, Party Data provided by SEC Parties which is not marked as confidential shall be treated as not being confidential and as such shall not be subject to any of the provisions described within this Policy nor shall the Panel (or its Sub-Committees and Working groups, SECCo and SECAS) be subject to any confidentiality obligations.

7.3 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 Annex A.

7.4 Handling

Where a SEC Party has marked its Party Data as confidential (or, where provided by the DCC, 'confidential'), 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[3)] 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[4)] 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~~ permitted under the Code;
- required under the Laws and Directives;
- ~~and/or~~ requested by the Authority;

[2] Other than as a result as a breach by the Panel.
[3] The Panel have procured a secure file hosting platform for the purposes of securely fulfilling their duties under Sections G, I and L of the SEC. More information on the platform is available here.

- to do so has been explicitly ~~received~~ permitted ~~from~~ by 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.

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.

7.5 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;
- any confidential Party Data which is required to be accessible by Panel Members, Sub-Committees or Working Groups (including via SECAS or SECCo) shall be stored on Egress with access restricted to named, authorised individuals and downloading of such Data shall only be permitted by Panel Members;
- Panel Members shall not make hard copies of any confidential Party Data which they have downloaded;
- any confidential Party Data that is distributed to Panel Members, Sub-Committee Members or Working Group members, must be done so via 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.

7.6 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[4], 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 document which will ensure a review of the retention requirements;
- retention conditions shall be designed to protect records against unauthorised access, loss, falsification, destruction and theft; and
- 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 Annex B.

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Appendix A: DCC Classifications

This appendix describes the classifications available to the DCC, as per the Code, and the associated provisions. As this covers the DCC providing information to SEC Parties, this section does not include handling, storage or retention policies.

Where the Panel (and its Sub-Committees and Working Groups, SECAS, ~~and~~ SECCo and the Authority) is in receipt of DCC confidential or controlled Data it shall be subject to the measures described in section 7 of this Policy.

1. Classifications

1.1 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).

1.1.1 Confidential Liability

Each SEC Party's Liability for breaches of data marked as confidential shall be unlimited in accordance with SEC Section M2.3.

1.2 Controlled

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 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).

1.2.1 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 Public

Whilst not a Code defined marking, the DCC makes use of a 'public' marking, indicating that the information in question is considered neither 'controlled' nor 'confidential'.

1.4 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.

1.5 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.

1.6 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’[5]. Therefore, if a SEC Party wishes to receive confidential or controlled DCC Data they should do so in accordance with the provisions below.

1.6.1 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 listing of names and contact details of individuals who are authorised by it to receive such Data. The DCC 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).

Requests for access to confidential data should be made via servicedesk@smartdcc.co.uk.

[5] Subject to exemptions stated in SEC Section M4.20

1.6.2 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.

Appendix B: SEC Governance Classification Rules

This appendix describes the classifications available to the Panel, its Sub-Committees and Working Groups, SECCo and SECAS. 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 7.1 of the body of this Policy, as defined in SEC Section M4. Non-binding sub-categorisations are also set out in Annex A.

1. Panel, Sub-Committees and Working Groups, SECAS and SECCo

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	
RED	Non-disclosable information and Restricted to Panel/Sub-Committee Members/Working Group Members (including alternates). Participants must not disseminate the information outside of the governance group. RED information may only be discussed during a meeting where all participants present have signed a declaration form, stating their acceptance to abide by these terms. RED information should not be discussed with anyone who is not a member of the governance group. Agenda items marked as RED will be discussed in a closed, confidential session and discussions will only be included in minutes marked as RED. Information classified as RED may be disclosed to the Panel (or any other element of the SEC governance structure) but only following approval by the committee in question. Any RED information discussed by the Panel in this manner shall also be subject to the same non-disclosure provisions. Any documentation classified as RED shall be distributed using the agreed secure storage and distribution platform.
AMBER	Limited disclosure and Restricted to Sub-Committee Members/Working Group members, the Panel and those who have a need to know in order to take action. Panel, Sub-Committee and Working Group members may share the information with other organisations belonging to the same SEC Party Category. Where information is deemed to be relevant to organisations who are not represented at a Panel, Sub-Committee and Working Group meeting, the Chair may direct that SECAS provide this information to a wider group of stakeholders.

Classification	
	Agenda items marked as AMBER will be discussed in a closed, confidential session and discussions will only be included in the minutes marked as AMBER.
GREEN	Information can be shared with other SEC Parties and SMIP stakeholders[6] at large but not made publicly available. "Green" will be the default classification for any discussions unless otherwise notified. Agenda items marked as GREEN will be included in the minutes marked as green.
WHITE	Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member may publish the information, subject to copyright. Agenda items marked as WHITE will be included in the minutes marked as white.

Table 1: Classification Table

1.1 Confidentiality and Disclosure Agreement

With the exception of the Authority and representatives of the Secretary of State, ~~A~~all members 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. The agreement states that they have understood the relevant Terms of Reference, all of which will include the classification table above and state that they understand the information sharing levels confidentiality and disclosure obligations.

1.2 Egress

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 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. The Egress Switch secure workspace has the following security features and classifications[7]:

- secures data at rest and in transit using AES-256 bit encryption;
- utilises FIPS 140-2 certified libraries;
- secure authentication and user enrolment;
- CESG CPA Foundation Grade certified encryption product;
- CESG Pan Government Accreditation;
- ISO 27001:2013 accredited;
- Cyber Essentials Plus certified;
- Skyhigh Cloud Trust™ rating of Enterprise-Ready;

[6] For example: device manufacturers, smart metering network security, information assurance or Critical National Infrastructure (CNI) community. Please note that the wording of this classification is subject to change once the SMIP has completed.
[7] https://www.egress.com/what-we-offer/secure_workspace_datasheet_egress_switch-pdf/download

- uses data centres accredited to ISO 27001/9001; and
- listed under Cyber Security Supplier to Government Scheme.

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.

Annex A – SEC Panel Information Classification and Handling Matrix

Please note that the labelling and handling directions provided below are for *example only* and materials marked in any other manner (provided the marking is clear and visible) shall still be subject to the provisions detailed in section 7 of this Policy.

Labelling and Handling	Unmarked Guidelines	Confidential Guidelines
Document Labelling	No marking required	Any documentation provided to SECAS should have clear labelling applied to the footer of every page of the document. All pages should be numbered. In addition to this, the document title should be prefixed with CONFIDENTIAL.
Portable Media Labelling	No marking required	Any portable media provided to SECAS should have clear labelling applied to the footer of every page of the document contained on said portable media. All pages should be numbered. In addition to this, the document title should be prefixed with CONFIDENTIAL.
Internal Distribution - Hardcopy	None	Any documentation provided to SECAS should have clear labelling applied to the footer of every page of the document. All pages should be numbered. In addition to this, the document title should be prefixed with CONFIDENTIAL.
External Distribution - Hardcopy	Check that information being distributed matches requirements. Ordinary envelope through public mail system.	SEC Parties shall ensure that envelopes are marked “Confidential”. Any documentation contained within, when provided to SECAS, should have clear labelling applied to the footer of every page of the document. All pages should be numbered. In addition to this, the document title should be prefixed with CONFIDENTIAL.

Labelling and Handling	Unmarked Guidelines	Confidential Guidelines
External Distribution - Softcopy (USB, CD, DVD etc)	Check that information being distributed matches requirements. Ordinary envelope through public mail system.	SEC Parties shall ensure that envelopes are marked “Confidential”. Any documentation provided to SECAS should have clear labelling applied to the footer of every page of the document. All pages should be numbered. In addition to this, the document title should be prefixed with CONFIDENTIAL.
Email	Check that information being emailed matches requirements. No requirements.	In the instance of emails, the classification label should be included in the email subject and at the top of the body of the email itself. Subject CONFIDENTIAL: Party Data Email

Annex B: Retention and Destruction of Data by the Panel

Labelling and Handling	Unmarked	Confidential
Physical Storage	No requirements.	Information assets shall be stored in as few places as possible and archived or destroyed when no longer required in line with Code and/or SECAS retention policy requirements[8]. Party Data that has the potential to be stored on a long-term basis shall be kept in a secure location with access restricted to those with a business requirement.
Network Storage	No requirements.	Information assets shall be stored in as few places as possible and archived or destroyed when no longer required in line with Code and/or SECAS retention policy requirements. Party Data that has the potential to be stored on a long-term basis shall be kept in a secure location with access restricted to those with a business requirement. Any confidential Party Data which is required to be accessible by Panel Members/Sub-Committee Members/Working Groups/SECAS employees shall only be stored on Egress and downloading of such Data shall only be permitted by Panel Members. Panel Members shall not make hard copies of any confidential Party Data which they have downloaded. Any confidential Party Data that is distributed to Panel Members/Sub-Committee Members/Working Groups/SECAS employees must be done so via secure, encrypted email, and destroyed within 5WD of receipt, or after the relevant committee meeting.

[8] BS EN 15713:2009 - Secure Destruction of Confidential Material Code of Best Practice;
CPNI Secure Destruction Sensitive information - Government related information;

Labelling and Handling	Unmarked	Confidential
Telephone / Video Conferencing	No requirements.	Panel Members/ Sub-Committee Members/ SECAS employees should always be conscious of their surroundings when engaged in confidential conversations (i.e. verbal exchange of SSC information via telephone, video conference, WebEx etc.) or when reviewing/ displaying information on their Laptop outside of their office environment.
Destruction of Paper	No requirements - recycle where possible.	When information is no longer required for business purposes, 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.
Removal / Destruction of Data from Portable Storage Media	Portable storage media must be disposed of in accordance with the WEEE Directive after all the data on the drives has been deleted.	When information is no longer required for business purposes, 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.
Removal / Destruction of Data from PCs, Laptops and other Hardware	PCs, laptops, servers and other hardware must be disposed of in accordance with the WEEE Directive after all the data on the drives has been deleted.	When information is no longer required for business purposes, 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.