**Version AG 1.~~1~~2**

# Appendix AG

# Incident Management Policy

## Definitions

In this document, except where the context otherwise requires:

- Expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section;
- The expressions in the left hand column below shall have the meaning given to them in the right hand column below; and
- References throughout to Service Desk mean the DCC via the Service Desk.

| | |
|---|---|
| **Business Continuity Event** | An Event, other than a Disaster, that causes one or more of the 'DCC BC Impacts' listed in Table 4 of this document. |
| **CPNI** | Centre for the Protection of National Infrastructure |
| **Code of Connection** | One of the following Subsidiary Documents: DCC Gateway Connection Code of Connection; DCC User Interface Code of Connection; Registration Data Interface Code of Connection; Self Service Interface Code of Connection; SMKI Code of Connection; SMKI Repository Code of Connection; DCCKI Code of Connection; DCCKI Repository Code of Connection. |
| **Error Handling Strategy** | The procedures to be followed and actions to be taken where a Service Request or the commands or responses related to it fail to provide the result expected from that type or category of Service Request as further described in clause 4 |
| **HMG** | Her Majesty's Government |
| **Interested Party** | A Party or Registration Data Provider that is or has the potential to be affected by a Problem or Incident |
| **Known Error** | A fault in a component of the DCC Total System which is used for the provision of Live Services, identified by the successful diagnosis of an Incident or Problem and for which both Root Cause and a temporary work-around or a permanent solution have been identified |

| | |
|---|---|
| **Live Service** | Means<br>1) any of the Services that the DCC is obliged to provide to a User, an Authorised Subscriber, a DCC Gateway Party (once its connection is capable of operation), but excluding Testing Services as set out in H14, and<br>2) the exchange of data pursuant to Section E2. |
| **Nominated Individual** | Means an individual who has been nominated by an Incident Party in accordance with clause 1.4.5 of this Incident Management Policy |
| **Root Cause** | is the ultimate cause of an Incident or Problem |
| **Root Cause Analysis** | a class of problem solving methods aimed at identifying the Root Cause of a Problem or Incident |
| **Service Alert** | An alert notifying Interested Parties of a current issue which may impact the provision of Services |
| **Target Initial Response Time** | The time period within which an Incident within each Category should be recorded on the Incident Management Log and assigned to a resolver |

**Contents**


1 **Introduction** **5**

1.1 Purpose 5

1.2 Background 5

1.3 Scope 5

1.4 General Provisions **5**

2 **Incident Management** **8**

2.1 Pre-requisites to Raising an Incident 8

2.2 Raising an Incident 9

2.3 Required Information 9

2.4 Incident Prioritisation & Categorisation 10

2.5 Incident Assignment 13

2.6 Identifying Interested Parties 15

2.7 Communications 15

2.8 Incident Escalation 15

2.9 Escalation Process 16

2.10 DCC Major Incidents and Major Security Incidents 17

2.11 Major Incidents not Assigned to the DCC 18

2.12 Incident Closure 19

2.13 Re-opening Closed Incidents 20

2.14 Re-occurring Incidents 20

3 **Problem Management** **21**

3.1 Opening a Problem 21

3.2 Prioritisation and Timescale for Closure of Problems 21

3.3 Closing a Problem 22

4 **Error Handling Strategy** **23**

5 **Business Continuity & Disaster Recovery** **24**

5.1 BCDR General Provisions 24

5.2 Business Continuity and Disaster Recovery Procedures 25

# 1. Introduction

## 1.1 Purpose

1.1.1 This document details the Incident Management Policy in accordance with the requirements of Section H9. It deals with the management of Incidents, including those related to Registration Data.

1.1.2 Additionally, clauses 4 and 5 cover the Error Handling Strategy and Business Continuity and Disaster Recovery respectively.

## 1.2 Background

1.2.1 The subject matter of this document is closely related to that of the Incident Management aspects of the Registration Data Interface Specification. In order to ensure an integrated solution to managing Incidents, certain common aspects of Incident Management are set out in this document and cross-referred to in the Registration Data Interface Specification.

1.2.2 The timetable for Registration Data refreshes is set out in the Registration Data Interface Code of Connection and the Registration Data Incident types are set out in the Registration Data Interface Specification.

1.2.3 Error conditions and how they should be handled are covered in clause 4, the Error Handling Strategy.

## 1.3 Scope

1.3.1 The Incident Management Policy details the full Incident Management lifecycle including management and declaration of Major Incidents, Problems and escalations.

## 1.4 General Provisions

1.4.1 Incidents may be raised only by the DCC or an Incident Party and in accordance with this Incident Management Policy.

1.4.2 Incidents raised and managed under this Incident Management Policy may relate to any Live Service. The Testing Issue Resolution Process set out in H14.37- H14.45 shall apply for the purpose of resolving Testing Issues.

1.4.3 In the event that an Incident Party considers it necessary to raise an issue relating to the provision of Services but which it considers outside the scope of Live Services or Testing Services, it shall contact the DCC directly and each of that Party and the DCC shall, acting reasonably, agree between them responsibility for resolution of the issue, which shall be resolved by the responsible Party as soon as reasonably practicable.

1.4.4 Incidents shall be raised and recorded in the Incident Management Log in accordance with clause 2.

1.4.5 Each Incident Party shall provide the DCC with, and shall subsequently provide the DCC with any changes to, a list of Nominated Individuals from their organisation who are authorised to:

a) contact the DCC to raise and record in the Incident Management Log an Incident and communicate with the DCC regarding the Incident; and/or

b) perform the roles identified in the escalation process defined in clause 2.9.

1.4.6 Each Registration Data Provider, when providing the DCC with a list of Nominated Individuals, shall provide details of both the core operating hours for the Registration Data Provider and the Registration Data Provider's out-of-hours facility.

1.4.7 Each Incident Party shall ensure that only its Nominated Individuals shall contact the DCC to raise an Incident.

1.4.8 The DCC shall ensure that only those Nominated Individuals pursuant to clause 1.4.5(a) shall raise an Incident.

1.4.9 The DCC shall implement an authentication procedure for confirming that a communication is from an Incident Party's Nominated Individual, and such procedure shall be commensurate with the risk to the Services and Data that would arise were someone other than a Nominated Individual to raise an Incident or obtain

information from the Service Desk. Incident Parties shall comply with this procedure.

1.4.10 The DCC and each Incident Party shall each ensure that information regarding Incidents and Problems is recorded and kept up to date in the Incident Management Log as follows:

a) for Major Incidents, the Incident Party shall comply with clause 2.2.2;

b) except in the case of clause 1.4.10 (a), the Incident Party shall use the Self Service Interface where it is able to do so and the DCC shall ensure that information provided in this way is automatically added to the Incident Management Log;

c) where the Incident Party is unable to use the Self Service Interface, it shall provide information to the Service Desk by email or by phone and the Service Desk shall ensure that this information is entered into the Incident Management Log;

d) when an Incident is submitted by email and the Incident Party does not provide the required information as detailed in clause 2.3, the Service Desk shall return an email to the Incident Party requesting the missing information and the Incident shall not be recorded in the Incident Management Log until the required information has been received by the Service Desk;

e) the Service Desk shall enter information that the DCC originates into the Incident Management Log;

f) the resolver shall ensure all actions to resolve the Incident are recorded in the Incident Management Log; and

g) In regard to items a) – f) above, the DCC and each Incident Party shall each ensure that information is as complete as is possible and is entered into the Incident Management Log as soon as is reasonably practicable.

## 2. INCIDENT MANAGEMENT

### 2.1 Pre-requisites to Raising an Incident

**DCC**

2.1.1 Before raising an Incident the DCC shall take all reasonable steps to ensure an Incident does not already exist for the issue.

2.1.2 Pursuant to Section E2.13, prior to the DCC raising an Incident regarding the provision of Registration Data by a Registration Data Provider, the DCC shall take all reasonable steps to confirm that the issue does not reside within the DCC System or processes.

**Incident Parties other than Registration Data Providers**

2.1.3 For the purposes of this clause 2.1.3 and clause 2.1.4, references to "Incident Party" do not include Registration Data Providers.

Before raising an Incident with the DCC the Incident Party shall take all reasonable steps to:

a) where appropriate, confirm that the issue does not reside within the HAN, or the Smart Meter, or other Devices which the Incident Party is responsible for operating;

b) confirm that the issue does not reside within the Incident Party's own systems and processes;

c) follow the guidance set out in the self-help material made available by the DCC, including checking for Known Errors and the application of any workarounds specified; and

d) where the party is a User and to the extent that this is possible, use the SSI or submit a Service Request to resolve the Incident in accordance with Section H9.2.

2.1.4 In the event that the activities in clause 2.1.3 have been completed and an Incident is to be raised with the DCC, where it has access to the Self-Service Interface, the Incident Party shall check on the Self Service Interface to establish whether an Incident has already been raised or a Service Alert issued for this issue and:

a) in the event that the Incident Party can reasonably determine that an Incident or Service Alert for this issue exists, the Incident Party shall notify the Service Desk who shall register the Incident Party as an Interested Party within the Incident Management Log;

b) in the event that the Incident Party cannot identify an existing Incident or Service Alert they shall progress to clause 2.2 to raise an Incident.

**Registration Data Provider**

2.1.5 Prior to raising an Incident regarding the provision of data to and by the DCC, the Registration Data Provider shall take all reasonable steps to confirm that the issue does not reside within the Registration Data Provider's systems and processes.

## 2.2 Raising an Incident

2.2.1 Incidents can be raised at any time as set out in in clause 2.2.3, but only once the steps in clause 2.1 have been followed.

2.2.2 Where an Incident Party believes that an Incident meets the criteria of a Category 1 Incident (see clause 2.4.4), the Incident Party shall call the Service Desk as soon as reasonably practicable.

2.2.3 An Incident Party shall raise what it considers to be Category 2, 3, 4 and 5 Incidents as set out in clause 1.4.10 and provide information as set out in clause 2.3.1.

## 2.3 Required Information

2.3.1 When raising an Incident, the DCC or Incident Party shall provide the following information:

a) Contact name;

b) Contact Organisation;

c) Contact details;

d) Organisation's Incident reference number (where available);

e) Date and time of occurrence;

f) MPxN or Device ID (where appropriate);

g) Summary of Incident;

h) Business impact; and

i) Results of initial triage and diagnosis including references to existing Incidents, where appropriate, and details of investigations performed to satisfy pre-requisites set out in clause 2.1.

## 2.4 Incident Prioritisation and Categorisation

2.4.1 The DCC shall assign an Incident Category to an Incident raised by an Incident Party based on the information available at the time the Incident is recorded in the Incident Management Log.

2.4.2 The DCC shall assign an Incident Category to an Incident raised by the DCC using information available to the DCC at the time the Incident is recorded in the Incident Management Log.

2.4.3 The DCC shall progress the resolution of Incidents in priority order. The DCC shall determine the priority of an Incident by considering the Incident Category and the time remaining until the Target Resolution Time, as defined in clause 2.4.4.

### Categorisation Matrix

2.4.4 The DCC shall, acting reasonably, assign a Category to an Incident, having regard to the table below. The table further details the Target Resolution Time in accordance with Section H9.1(c).

| Incident Category | Description | All Incidents except those that pertain to the SMETS1 SM WAN to the extent that Vodafone Limited is the relevant DCC Service Provider | | Incidents that pertain to the SMETS1 SM WAN to the extent that Vodafone Limited is the relevant DCC Service Provider | |
|---|---|---|---|---|---|
| ~~Incident Category~~ | ~~Description~~ | **Target Initial Response Time** | **Target Resolution Time** | **Target Initial Response Time** | **Target Resolution Time** |
| 1 | A Category 1 Incident (Major Incident) is an Incident which, in the reasonable opinion of the DCC:<br>• prevents a large group of Incident Parties from using the Live Services;<br>• has a critical adverse impact on the activities of the Incident Parties using the Live Services of the DCC;<br>• causes significant financial loss and/or disruption to the Incident Parties; or<br>• results in any material loss or corruption of DCC Data.<br>For a Major Security Incident there are additional considerations:<br>• HMG, through CPNI, have declared a | 10 minutes | 4 hours | N/A | 7 hours |

| | | | | | |
|---|---|---|---|---|---|
| | Major Incident based on their procedures;<br>• a pattern has been seen across the DCC Total System that in total would have a significant security impact; or<br>• Data covered by the Data Protection ~~Legislation~~Act has either been lost or obtained by an unauthorised party, or is seriously threatened. | | | | |
| 2 | An Incident which in the reasonable opinion of the DCC:<br>• has a non-critical adverse impact on the activities of Incident Parties, but the Live Service is still working at a reduced capacity; or | 20 minutes | 24 hours | N/A | 17 hours |

| | | | | | |
|---|---|---|---|---|---|
| 3 | An Incident which, in the reasonable opinion of the DCC:<br>• has an adverse impact on the activities of an Incident Party but which can be reduced to a moderate adverse impact due to the availability of a workaround; or<br>• has a moderate adverse impact on the activities of an Incident Party. | 45 minutes | 72 hours | N/A | 17 hours |
| 4 | An Incident which, in the reasonable opinion of the DCC has a minor adverse impact on the activities of an Incident Party. | 3 hours | 5 days | N/A | 9 days |
| 5 | An Incident which, in the reasonable opinion of the DCC has minimal impact on the activities of Incident Party. | 1 day | 10 days | N/A | 9 days |

Table 1 - This table covers all Incident categories including Security Incidents.

2.4.5 If an Incident Party believes an Incident has been allocated an incorrect Incident Category by the DCC or has been subsequently updated to an incorrect Incident Category by the DCC, it may invoke the escalation process set out in clause 2.9.

2.4.6 The DCC may change the Incident Category of an Incident if more information becomes available. The DCC shall provide to Interested Parties, through a Nominated Individual, details of why the Incident Category has been changed. The DCC shall update the Incident Management Log with the revised Incident Category.

## 2.5 Incident Assignment

2.5.1 The Service Desk shall manage Incidents recorded in the Incident Management Log through the Incident lifecycle.

2.5.2 The Service Desk shall assess the Incident and assign resolution activities to the appropriate resolver in accordance with Section H9.2, and the resolver may be the DCC or an Incident Party.

2.5.3 In the event that Incident resolution activities are assigned to a Registration Data Provider at a time which falls outside of the Registration Data Provider's hours of operation, and where the DCC has classified the Incident as a Category 1 or 2, the DCC shall contact the Registration Data Provider via its out-of-hours facility as provided in accordance with the clause 1.4.6.

2.5.4 In the event that Incident resolution activities are assigned to a Registration Data Provider at a time which falls outside of the Registration Data Provider's hours of operation and the DCC has classified the Incident as a Category 3, 4 or 5, the DCC shall contact the Registration Data Provider when their business operations commence on the next Working Day. In such instances the time during which the Registration Data Provider was not able to be contacted shall be disregarded for the purpose of calculating the resolution time for the Incident.

2.5.5 Pursuant to H9.8 the resolver assigned to an Incident shall perform the appropriate steps to resolve the Incident in accordance with Section H9.8, and shall record information as set out in clause 1.4.10.

2.5.6 When assigning an Incident to an Incident Party where the DCC requires the Incident Party to diagnose or confirm resolution of an Incident, the DCC shall:

a) engage with the Incident Party through a Nominated Individual;

b) set the Incident status to pending; and

c) assign the activity to the Incident Party, and the resolution time shall not include the period of time during which the Incident is assigned to the Incident Party.

2.5.7 The Incident Party shall, using a reasonable mechanism, confirm to the DCC when all activities requested pursuant to clauses 2.5.5 are complete, providing details of steps taken, which the Service Desk shall ensure are included in the Incident Management Log. The DCC shall then reassign the Incident or update the status in the Incident Management Log to resolved, as appropriate, based on the information received.

2.5.8 Where an Incident has been investigated but has subsequently been determined not to be an Incident:

a) the Service Desk shall contact the Incident Party that raised the Incident through a Nominated Individual and provide the relevant information that the DCC holds to enable the Incident Party to raise and manage the Incident within its own system; and

b) the Service Desk shall set the status of the Incident in the Incident Management Log to closed.

2.5.9 If an Incident Party identifies that an Incident has been assigned to it but it should not be responsible for resolving it, the Incident Party shall advise the Service Desk, providing supporting information, and the DCC shall investigate and re-assign as appropriate.

2.5.10 The DCC shall collate and make available to Network Parties and the Panel data related to the time taken to resolve Incidents associated with the exchange of data pursuant to Section E of the Code, where the DCC is responsible for resolving the Incident but in order to do so, activity must be undertaken by a Registration Data Provider.

## 2.6 Identifying Interested Parties

2.6.1 The Service Desk shall take all reasonable steps using information available from the Live Services including Incident data, as appropriate, to identify Interested Parties for an Incident.

2.6.2 The DCC shall inform the Interested Parties identified by the DCC of the Incident through a Nominated Individual**.**

## 2.7 Communications

2.7.1 Throughout the lifecycle of the Incident, the DCC, via the Service Desk, shall communicate updates to the Incident Party or other identified Interested Parties. These communications may be via email, phone call and/or via updates to the Incident Management Log.

## 2.8 Incident Escalation

2.8.1 The rules and process for the escalation of an Incident are detailed in this clause and clause 2.9.

2.8.2 The DCC and Incident Party shall adopt the escalation process as defined in clause 2.9 to ensure that Nominated Individuals and DCC representatives with the necessary authority and the appropriate resources are applied to resolving the Incident.

2.8.3 The Service Desk shall monitor Incidents throughout their lifecycle and automatic reminder notifications shall be sent to appropriate resolvers based on Incident Category, Target Initial Response Time and Target Resolution Time.

2.8.4 Subject to clause 2.8.5, the Incident Party that raised an Incident with the Service Desk, an Interested Party, or an Incident Party to which the Incident has been subsequently reassigned by the DCC, may request that the Incident is escalated.

2.8.5 Incidents may be escalated under the following circumstances:

a) disagreement with categorisation;

b) Target Initial Response Time has not been met;

c) Target Resolution Time about to be exceeded;

d) lack of appropriate response;

e) dissatisfaction with the progress of an assigned activity;

f) dissatisfaction with the progress of an Incident; or

g) dissatisfaction with the resolution of an Incident.

2.8.6 The Service Desk shall include full details of the escalation in the Incident Management Log.

## 2.9 Escalation Process

2.9.1 Escalated Incidents shall be progressed in accordance with the table below. All escalations shall follow the process and adhere to the sequential order.

| Level | DCC | Incident Party |
|---|---|---|

| | | |
|---|---|---|
| **L1 Escalation** | Service Desk | Individual nominated to act in the role of service desk operator in accordance with clause 1.4.5 |
| **L2 Escalation** | Service Desk Manager | Individual nominated to act in the role of service desk manager in accordance with clause 1.4.5 |
| **L3 Escalation** | Service Manager | Individual nominated to act in the role of Service Manager in accordance with clause 1.4.5 |
| **L4 Escalation** | Head of Service | Individual nominated to act in the role of Head of Service in accordance with clause 1.4.5 |
| **L5 Escalation** | Operations Director | Individual nominated to act in the role of Operations Director in accordance with clause 1.4.5 |

Table 2 – Escalation Process

2.9.2 If, following a Level 5 escalation, a resolution cannot be satisfactorily agreed between the DCC and the escalating organisation, the Incident may be escalated by any Interested Party to the Panel and Section H9.16 shall apply.

2.9.3 The DCC and escalating Incident Party shall provide appropriate evidence to the Panel that it has been through all earlier escalation levels before escalating an Incident to the Panel.

## 2.10 DCC Major Incidents and Major Security Incidents

2.10.1 All Category 1 Incidents shall also be treated as Major Incidents. Major Security Incidents shall also be treated as Category 1 Incidents.

2.10.2 Once an Incident has been reported to the Service Desk pursuant to clause 2.2.2, the Service Desk shall perform initial triage on the Incident. The Major Incident management process and/or the DCC security team shall be engaged to progress and resolve the Incident where triage confirms that the DCC believes that the Incident should be treated as a Category 1 Incident, unless the circumstances set out in 2.10.7 apply.

2.10.3 If an Incident is updated to become a Category 1 Incident the provisions of this clause 2.10 will also apply.

2.10.4 The DCC shall notify all Incident Parties that are likely to be affected by such Major Incident by a reasonable means in accordance with Section H9.11.

2.10.5 On resolution of the Major Incident, the DCC shall raise a Problem to confirm the Root Cause.

2.10.6 The DCC shall make the details from the Problem available to Interested Parties.

2.10.7 Where a Major Incident has been investigated but then turns out to be an Incident which the DCC is not responsible for resolving (as set out in H9.2(b)) then the Service Desk shall:

a) Contact the appropriate Incident Party through a Nominated Individual;

b) assign the Incident to the Incident Party; and

c) set the Incident status to pending.

2.10.8 Where a Major Incident has been investigated but turns out not to be an Incident:

a) the Service Desk shall contact the Incident Party that raised the Incident through a Nominated Individual and provide the details to enable the Incident Party to raise and manage the incident within their own system; and

b) the Service Desk shall set the status of the Incident to closed.

**Major Security Incidents**

2.10.10 Clauses 2.10.11 and 2.10.12 shall apply for a Major Security Incident.

2.10.11 The Incident Party shall notify the Panel, the Security Sub-Committee, in accordance with Section G3, and, pursuant to section H9, the DCC if:

a) it detects a security Incident within its environment of which the DCC needs to be informed; or

b) any potential Security Incident it detects appears to relate to the DCC Total System.

2.10.12 The DCC shall notify the Panel and the Security Sub- Committee, in accordance with Section G2, and, pursuant to Section H9, shall inform an Incident Party by an appropriate mechanism if:

a) any Security Incident occurs that is identified in the Code as requiring notification to the Incident Party or the Panel and Security Subcommittee; or

b) a Security Incident indicates a breach of the provisions of a Code of Connection.

## 2.11 Major Incidents not Assigned to the DCC

2.11.1 In the event that a Major Incident is assigned to an Incident Party other than the DCC:

a) the Incident Party may request that the DCC provides reasonable assistance. When this is requested the DCC shall provide all reasonable assistance to the Incident Party responsible for resolving the Incident in accordance with Section H9.12(b); and

b) as part of such reasonable assistance, the DCC may disseminate the information to Incident Parties if requested by the Incident Party, using the Self Service Interface and other mechanisms as appropriate.

## 2.12 Incident Closure

2.12.1 The rules for the closure of Incidents are detailed below.

2.12.2 An Incident that the DCC is responsible for resolving shall be resolved by the DCC in accordance with the Target Resolution Times set out in the categorisation matrix in clause 2.4.

2.12.3 The Service Desk and the resolver shall each record details of all steps they have each taken to resolve the Incident in the Incident Management Log, as set out in clause 1.4.10.

2.12.4 The Service Desk shall notify the Incident Party and/or other Interested Parties and the resolver via email when the DCC sets the Incident status to resolved.

2.12.5 If the Incident is resolved through the application of a workaround, the Service Desk shall either raise a new Problem or the Incident shall be associated with an existing Problem where one exists.

2.12.6 If it does not consider that the Incident is resolved, the Incident Party, resolver or an Interested Party shall respond to the Service Desk via email or phone call within 3 Working Days, unless a longer period has been agreed by the Service Desk, such agreement to not be unreasonably withheld. In so doing, the relevant party shall provide supporting information as to why they consider the Incident not to be resolved. Then:

a) If the Service Desk receives, with supporting information, a response detailing that the Incident is not resolved, the Service Desk will change the status from resolved and reassign the Incident for investigation in accordance with Section H9; or

b) If a response is not received from the Incident Party within the aforementioned timeframe the Service Desk shall close the Incident.

2.12.7 In the event that the Incident Party requires subject matter expert advice before confirming closure and the subject matter expert is unavailable, the Incident Party may contact the Service Desk via email or phone call to request that the closure period be extended.

2.12.8 In the event that the Incident is the result of an intermittent issue the Service Desk shall apply what it reasonably deems to be an appropriate closure period based on the frequency of the occurrences of the issue, and shall close the Incident after this period has elapsed without any further occurrences. The Service Desk shall record this in the Incident Management Log.

2.12.9 After the Incident has been resolved, the Service Desk may raise a Problem and link it to the Incident.

## 2.13 Re-opening Closed Incidents

2.13.1 The Incident Party that originally raised an Incident may only re-open it if it was closed with a workaround and one of the following circumstances occurs:

a) the workaround fails; or

b) the workaround deteriorates to a point that it affects normal business operations.

2.13.2 If a Problem associated with an Incident has been closed, it shall not be possible to re-open the Incident. In this case, the Incident Party shall raise a new Incident.

## 2.14 Re-occurring Incidents

2.14.1 If a previous Incident reoccurs after it has been closed in line with the procedures in this Incident Management Policy, the Incident Party shall raise a new Incident, in accordance with the provisions set out above.

2.14.2 The DCC may identify re-occurring Incidents by performing trending, correlation and incident matching. Confirmed re-occurrences may be progressed through Problem management.

2.14.3 An Incident Party may identify a re-occurring incident and may notify the DCC. In so doing, the Incident Party shall provide all related Incident reference numbers to the DCC who may progress the issue through Problem management, as set out in clause 3.

# 3. PROBLEM MANAGEMENT

## 3.1 Opening a Problem

3.1.1 The DCC shall open a Problem in the Incident Management Log in the following circumstances:

a) when a Major Incident has been resolved;

b) when an Incident is closed with a workaround applied; or

c) when the DCC has identified a re-occurring Incident.

3.1.2 The DCC shall allocate a reasonable initial timescale for carrying out the Root Cause Analysis to enable the re-classification of the Problem as a Known Error.

## 3.2 Prioritisation and Timescale for Closure of Problems

3.2.1 The DCC shall periodically issue and make available a report listing open Problems to Incident Parties and the Panel.

3.2.2 The report shall set out for each open Problem:

a) date opened;

b) Problem classification;

c) Problem status;

d) the target closure date;

e) the anticipated costs (in DCC's reasonable opinion) for the investigation and resolution of the Problem, where appropriate;

f) the anticipated timescales for the closure of a Problem;

g) the likely impact on the DCC's business, and its effects on Incident Parties of closing a Problem and continuing with a workaround, highlighting instances where implementing a permanent solution may not be the recommended approach; and

h) the reason for any target closure date change.

3.2.3 Following the issuing of such a report, the DCC shall discuss with Incident Parties the prioritisation and preferred timescales for the progression of each Problem. Following discussion, and taking respondents' views into account, the DCC shall determine the prioritisation and preferred timescales for the progression of each Problem.

3.2.4 If a Problem investigation or resolution requires a change to the Code a Draft Proposal shall be submitted by the DCC.

## 3.3 Closing a Problem

3.3.1 The rules for closure of a Problem are detailed below, as required by Section H9.1(k).

3.3.2 Following the application of a permanent fix, the DCC shall discuss the outcome with Interested Parties before closing the Problem.

3.3.3 Details of all steps taken to close the Problem shall be recorded, as set out in clause 1.4.10.

3.3.4 The DCC shall only close a Problem once one of the following conditions has been met and the DCC has discussed this with Interested Parties that:

a) the permanent fix has been applied; or

b) an enhanced and acceptable workaround is in place; or

c) the DCC will not continue investigations.

## 4. ERROR HANDLING STRATEGY

4.1 The first version of the contents of the Error Handling Strategy will be the 'Error Handling Strategy – DCC Guidance Document' as published by the DCC in June 2016.

4.2 The DCC shall make the Error Handling Strategy available to Users through the Self Service Interface.

4.3 The DCC may update the Error Handling Strategy from time to time. The DCC shall ensure that Parties are consulted prior to making any changes to the Error Handling Strategy and take into account any relevant views expressed by Parties in making any changes to it.

# 5. BUSINESS CONTINUITY AND DISASTER RECOVERY

## 5.1 BCDR General Provisions

5.1.1 Users, Other Parties and Registration Data Providers shall ensure that the contact details provided to the DCC for the purposes of Incident notifications are up to date.

5.1.2 The DCC shall record and treat any Disaster as a Major Incident.

5.1.3 The DCC shall coordinate recovery actions for any Disaster in order to minimise the impact on Services.

5.1.4 The DCC shall notify Incident Parties of a Disaster, with details of the Major Incident and the expected duration of the outage, if any. The DCC shall further inform Incident Parties when Services are restored.

5.1.5 The DCC shall notify Incident Parties of any event that results in a disruption to the Services as set out in Table 4 of this document, with details of the expected duration of the outage, if any. The DCC shall further inform Incident Parties when Services are restored.

5.1.6 The DCC shall implement the processes and arrangements outlined in the tables in clause 5.2 in order to meet the requirements as detailed in Section H10.13.

5.1.7 When requested by the DCC, upon restoration of Services, Incident Parties shall confirm that Services are fully restored.

5.1.8 Upon restoration of Services, if an Incident Party continues to have loss of Services they shall follow the incident management process steps outlined in clause 2.1.

## 5.2 Business Continuity and Disaster Recovery Procedures

### Disaster Recovery

5.2.1 Pursuant to the requirements of Section H10.9:

a) the DCC shall implement the measures in the table below under 'DCC Mitigation' to reduce the likelihood of the Disaster occurring and limit the impact in the event that a Disaster has occurred;

b) in the event of a Disaster, the DCC shall follow the actions in the table below detailed under 'DCC Recovery Action'; and

c) Incident Parties may experience the impact set out in the table below under 'Incident Party Impact' and shall follow the actions as detailed under 'Incident Party Actions on failure, failover or failback'.

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D1(a) | The DCC loses the primary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence. | The DCC shall provide primary and secondary data centres providing data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties may experience a loss of all Services on failover to the secondary data centre and on failback to the primary data centre, with the exception of some Testing Services which operate from the secondary data centre. | 1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored.<br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed).<br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and ~~D15~~D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D1(b) | The DCC loses the primary data centre provided pursuant to the SMETS1 Data Services contract(s). | The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on failback to the primary data centre. | 1. Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).<br>2. | SMETS1 |
| D2 | The DCC loses the secondary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence. | The DCC shall provide the ability to deliver Testing Services from either the secondary or primary data centres.<br><br>All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) recover Services at the primary data centre; or<br><br>b) recover Services at the secondary data centre. | Incident Parties will experience a loss of some Testing Services.<br><br>Incident Parties may experience a loss of some data within Testing Services. | 1. When requested by the DCC, Incident Parties shall suspend the use of Testing Services until notified that Services have been restored.<br><br>2. Upon Services restoration, Incident Parties may resubmit failed test messages. | SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D3(a) | The DCC loses both the primary and secondary data centres provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence. | The DCC shall ensure that all configurations & data are backed up & backups are stored offsite. | The DCC shall do one or more of the following:<br><br>a) recover Services at the primary data centre;<br><br>b) recover Services at the secondary data centre;<br><br>c) restore Services to new infrastructure at an alternative data centre;<br><br>d) set up network links to the new data centre; | Incident Parties may experience a loss of all Services.<br><br>Incident Parties may experience a loss of some transactions.<br><br>Some information related to billing and Service Levels may be lost.<br><br>On restart the DCC may impose systems-driven Restrictions on transaction volumes/types. | 1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored.<br><br>2. Upon Services restoration, Incident Parties may resubmit failed messages. | SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D3(b) | The DCC loses both the primary and secondary data centres provided pursuant to the SMETS1 Data Services. | The DCC shall ensure that all configurations & data are backed up & backups are stored offsite. | The DCC shall do one or more of the following:<br><br>a) recover Services at the primary data centre;<br><br>b) recover Services at the secondary data centre;<br><br>c) restore Services to new infrastructure at an alternative data centre;<br><br>d) set up network links to the new data centre; | Incident Parties may experience a partial loss of all SMETS1 Services.<br><br>Incident Parties may experience a loss of some SMETS1 transactions to a particular S1SP.<br><br>On restart the DCC may impose systems-driven Restrictions on transaction volumes/types. | 1. Upon restoration of impacted Services, Incident Parties shall resubmit any that have failed SMETS1 Service Requests. | SMETS1 |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D4 | DCC Services are impacted by a virus or malware | The DCC constantly monitors its environments and networks to ensure the integrity of firewalls and anti-virus measures. | The DCC shall do one or more of the following:<br><br>a) halt processing and clear the virus or malware;<br><br>b) failover to a secondary data centre (or primary data centre) in the case of Testing Services;<br><br>c) isolate the affected system and clear the virus or malware;<br><br>d) cease to process transactions from Incident Parties impacted by the virus or malware until confirmation is received that they have applied necessary measures;<br><br>e) apply any software patches to its Services; or<br><br>f) recover from backup. | Incident Parties may experience a loss or interruption to affected Services.<br><br>The DCC may impose systems-driven restrictions on transaction volumes/types on restart.<br><br>Additional impacts are detailed in column 5 of rows D2, D5 to D12 and D15 of this table. | 1. When requested by the DCC, Incident Parties shall suspend use of any affected Services.<br><br>2. Prior to re-commencement of Service provision, the DCC may request that each Incident Party confirms that it has cleaned its User Systems and applied necessary measures to prevent the virus or malware reoccurring.<br><br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | SMETS1 and SMETS2+ |

| Disaster ID | DCC ~~-~~Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D5 | The DCC's experiences a failure of the part of the DCC Systems responsible for delivering Service Requests, Commands, Responses & Alerts | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active- passive configuration between data centres.<br><br>All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties may experience a loss of Communication, Enrolment and Local Command Services.<br><br>Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre, during failover to the secondary data centre and failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend ~~submission of Service Requests and Signed Pre-Commands~~ until notified that Services have been restored~~.~~:<br><br>• in respect of SMETS2+, the submission of Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, the submission of SMETS1 Service Requests.<br><br>2. Upon restoration of impacted Services, Incident Parties may recommence submission ~~of Service Requests and Signed Pre-Commands~~ (including submitting any that have failed)~~.~~ of:<br><br>• in respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br><br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D8, D9, D10, D11 and ~~D15~~ D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | SMETS1 and SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D6 | Intentionally Left Blank | | | | | |
| D7 | Intentionally Left Blank | | | | | |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D8 | The DCC experiences a failure of the systems used to support the operation of the CoS Party. | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties would be unable to successfully send CoS Update Security Credentials Service Requests.<br><br>Incident Parties may experience a loss of all Services during the failover to the secondary data centre.<br><br>Incident Parties would also experience a loss of all Services on failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend ~~submission of Service Requests and Signed Pre-Commands~~ until notified that Services have been restored:~~.~~<br><br>• in respect of SMETS2+, the submission of Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, the submission of SMETS1 Service Requests.<br><br>2. Upon restoration of impacted Services, Incident Parties may recommence submission ~~of Service Requests and Signed Pre-Commands~~ (including submitting any that have failed) of:~~.~~<br><br>• in respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br><br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D9, D10, D11 and ~~D15~~D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | SMETS1 and SMETS2+ |

| Disaster ID | DCC ~~-~~Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D9 | The DCC experiences a loss of connectivity to one or more Incident Parties | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. There are resilient network links to the DCC User Gateway Connection with automatic rerouting between both data centres. | The DCC shall do one or more of the following:<br>a) recover connection at the primary data centre;<br>b) recover connection at the secondary data centre;<br>c) recover User connection. | Incident Parties will experience loss of connectivity to Services via the DCC User Gateway Connection. | 1. In the event of a Services interruption, when advised by the DCC, Incident Parties shall suspend submission ~~of Service Requests and Signed Pre-Commands~~ via the DCC User Gateway Connection until Services are restored~~.~~ of:<br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br>2. In the event of a Services interruption, when requested by the DCC, Incident Parties shall only submit Category 1 Incidents.<br>3. Upon restoration of impacted Services, Incident Parties may recommence submission ~~of Service Requests and Signed Pre-Commands~~ (including submitting any that have failed)~~.~~ of:<br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests. | SMETS1 and SMETS2+ |

| Disaster ID | DCC ~~-~~Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D10 | The DCC experiences a failure of the systems used to support the Self-Service Interface | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the DCC User Gateway Connection with automatic rerouting between both data centres. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties would experience loss of connectivity to Services via the Self Service Interface.<br><br>Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend ~~submission of Service Requests and Signed Pre-Commands~~ until notified that Services have been restored submission of :<br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br><br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed).<br><br>~~1.~~3. Incident Parties may need to log in to the Self Service Interface again.<br><br>4. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D11 and ~~D15~~ D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | SMETS1 and SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D11(a) | The DCC experiences a failure of the connection between the service providers referred to in paragraphs 1.2(a) and 1.2(b) of Schedule 1 of the DCC Licence (DCC WAN Gateway). | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.<br><br>Commands, Responses & Alerts shall be cached. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover connection at the primary data centre. | Incident Parties may experience a delay or failure in the processing of Service Requests, Commands, Responses and Alerts.<br><br>Incident Parties may experience a loss of all Services during the failover to the secondary data centre.<br><br>Incident Parties would also experience a short impact on all Services on failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored.<br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed).<br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10 and ~~D15~~ D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D11(b) | The DCC experiences a failure of the connection between the DSP and the SMETS1 Data Service Providers (SMETS1 Management Gateway). | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.<br><br>Commands, Responses & Alerts shall be cached. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover connection at the primary data centre. | Incident Parties may experience a delay or failure in the processing of Service Requests, Commands, Responses and Alerts.<br><br>Incident Parties may experience a loss of all Services during the failover to the secondary data centre. | Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed). | SMETS1 |
| D12 | Intentionally Left Blank | | | | | |
| D13 | The DCC loses its primary data centre provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence. | The DCC shall provide instances of the SMKI service infrastructure at primary & secondary SMKI data centres in an active-passive configuration with full data replication between sites and resilient network links to the Data Service Provider.<br><br>The DCC shall backup all SMKI configurations & data and shall store backups offsite. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties would be unable to request new Organisational or Device Certificates during failure, failover or failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend transmission of Certificate Signing Requests.<br><br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Certificate Signing Requests (including submitting any that have failed). | SMETS1 and SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D14 | The DCC loses both primary & secondary data centres provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence. | The DCC shall maintain full off-site configuration & data backups. | The DCC shall:<br><br>a) Restore failed services at one of the existing datacentres; or<br><br>b) restore failed Services to new infrastructure at an alternative data centre and shall then redirect network links to the alternate data centre. | Incident Parties may be unable to request new Organisational or Device Certificates. | 1. When requested by the DCC, Incident Parties shall suspend submission of Certificate Signing Requests until Services have been restored.<br>2. Upon Services restoration, Incident Parties may resubmit failed Certificate Signing Requests. | SMETS12 and SMETS2+ |
| D15(a) | The DCC loses both primary data centres provided pursuant to the DCO (Dual Control Organisation) contract. | The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>c) fail over to the secondary data centre; or<br><br>d) recover Services at the primary data centre. | Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on failback to the primary data centre. | 1. Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed). | SMETS1 |

| Disaster ID | DCC ~~-~~Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D15 (b) | The DCC loses both primary & secondary data centres provided pursuant to the (Dual Control Organisation) contract. | The DCC shall maintain full off-site configuration & data backups. | The DCC shall do one or more of the following:<br><br>e) recover Services at the primary data centre;<br><br>f) recover Services at the secondary data centre;<br><br>g) restore Services to new infrastructure at an alternative data centre;<br><br>h) set up network links to the new data centre; | Incident Parties will experience a loss of all SMETS1 Services.<br><br>Incident Parties may experience a loss of some SMETS1 transactions to a particular S1SP.<br><br>On restart the DCC may impose systems-driven Restrictions on transaction volumes/types. | 1. When requested by the DCC, Incident Parties shall suspend submission of all SMETS 1 Service Requests until Services have been restored.<br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed). | SMETS1 |
| ~~D15~~D16 | A failure of a connection or interface between one or more Registration Data Providers (RDP) and the DCC | There are resilient network links to the Registration Data Providers from both primary and secondary data centres. | The DCC shall do one or more of the following:<br><br>a) recover connection at the primary data centre;<br><br>b) recover connection at the secondary data centre;<br><br>c) recover connection to the Registration Data Provider; or<br><br>d) Send and receive Registration update by alternative (secure) means. | There may be a delay in the update of registration data on the DCC. This may cause some Service Requests to fail registration data checks even though the Party submitting them is an Eligible User. | 1. Upon service restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests.<br>2. When requested by the DCC, RDPs shall send and receive updates by alternative (secure) means. | SMETS1 and SMETS2+ |

| Disaster ID | DCC ~~-~~Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| ~~D16~~D17 | The DCC loses a data centre provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence. | The DCC shall provide primary & secondary sites for communication services data centres in an active-active configuration. All configurations & data are backed up and backups are stored offsite.<br><br>In the event of failure of one communications service data centre, Services would continue to be provided from the secondary data centre. | The DCC shall:<br><br>a) restore the provision of Impacted Services at the affected communications data centre; or<br><br>b) restore the provision of impacted Services at a new data centre. | There would be no impact on Incident Parties from a single communications service data centre failure.<br><br>Restoration of the existing data centre will not impact Incident Parties. | 1. No action would be required from Incident Parties to resolve this Incident.<br>2. Restoration of the existing data centre will not require action from Incident Parties. | SMETS1 and SMETS2+ |
| ~~D17~~D18 | The DCC loses both data centres provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence. | The DCC shall maintain full off-site configuration & data backups. | The DCC shall:<br><br>a) restore impacted Services to new infrastructure at the affected location(s); or<br><br>b) restore services at an alternative data centre(s) | Incident Parties may be unable to send Commands to Devices or receive Responses and Device Alerts via the DCC and will experience loss of some Services. | 1. When requested by the DCC, Incident Parties shall suspend submission ~~of Service Requests and Signed Pre-Commands~~ until notified that Services have been restored~~.~~ of:<br><br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br><br>2. Incident Parties shall also comply with all reasonable DCC requests to assist with prioritising & phasing back transmission of Service Requests and/or SMETS1 Service Requests. | SMETS1 and SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| ~~D18~~D19 | The service provided pursuant to the contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence experiences multiple access node failure.( Failure of a single access node would not be regarded as a DCC Disaster). | The DCC has significant, although not complete, overlap between access nodes.<br><br>The DCC shall ensure that access nodes are of a resilient design and that it has sufficient provision of mobile equipment and components spares to restore service within acceptable timescales. | The DCC shall:<br><br>a) deploy field maintenance and/or mobile equipment to restore Services. | Incident Parties may experience the failure of impacted Services directed to meters, Communications Hubs and Gas Proxy Functions in the affected area(s). | Upon Services restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests. | SMETS1 and SMETS2+ |
| ~~D19~~D20 | Communications Hub Product Recall | The DCC has more than one source for Communications Hubs.<br><br>Buffer stocks are held by the DCC and Communications Hub manufacturers. | The DCC shall:<br><br>a) determine the nature and extent of the problem; and<br><br>b) notify all Incident Parties of the extent of product recall required and effects on existing stocks and future supply. | This could result in Incident Parties diverting field staff to uninstall affected Communications Hubs, resulting in delays in installations.<br><br>It might also impact stocks and future supply. | Incident Parties shall provide reasonable assistance to the DCC in resolving issues. | SMETS2+ |
| ~~D20~~D21 | Loss of a site housing a DCC service function | The DCC shall have arrangements in place to resume all activityat an alternate location as part of its business continuity arrangements. | The DCC shall:<br><br>a) relocate the service function to the designated recovery site & shall restore service from there; or<br><br>b) Recover services at existing site | Incident Parties may be unable to contact the affected service function until it has been recovered at an alternate location. | There is no action required from Incident Parties. | SMETS1 and SMETS2+ |

| Disaster ID | DCC -Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D22 | | | | | | |

Table 3 – Disaster Recovery Procedures

Business Continuity

5.2.2 Pursuant to the requirements of Section H10.9:

a) the DCC shall implement the measures in the table below under ‘DCC Mitigation’ to reduce the likelihood of a Business Continuity Event occurring and limit the impact in the event that a Business Continuity Event has occurred;

b) in the event of the occurrence of a Business Continuity Event, the DCC shall follow the actions in the table below detailed under ‘DCC Recovery Action’; and

c) Incident Parties may experience the impact set out in the table below under ‘Incident Party Impact’ and shall follow the actions as detailed under ‘Incident Party Actions on failure, failover or failback’.

| Business Continuity ID | DCC BC Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback |
|---|---|---|---|---|---|
| B6 | The DCC experiences a failure of the systems used to support the provision of service management. | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre; and<br><br>c) the DCC Service Desk shall capture Incidents using another method until it regains access to the Service Management System. | Incident Parties may be unable to raise incidents or access incident information via the Self Service Interface.<br><br>Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre. | 1. When requested by DCC, Incident Parties may only submit Category 1 Incidents.<br><br>2. Upon Services restoration, Incident Parties may submit outstanding Incidents.<br><br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D15 of table 3 above and B6, B7 and B12 of this table 4, as relevant, when DCC fails over from or fails back to the primary data centre. |

| Business Continuity ID | DCC BC Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback |
|---|---|---|---|---|---|
| B7 | The DCC experiences a failure of the systems used to support the provision of data warehousing and reporting. | The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br><br>All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br><br>a) fail over to the secondary data centre; or<br><br>b) recover Services at the primary data centre. | Incident Parties may experience unavailability of preconfigured reports via the<br><br>Self Service Interface.<br><br>Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored.<br><br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed).<br><br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D15 of table 3 above and B6, B7 and B12 of this table 4, as relevant, when DCC fails over from or fails back to the primary data centre. |

| Business Continuity ID | DCC BC Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback |
|---|---|---|---|---|---|
| B12 | Loss of the systems used to support Communications Hub ordering. | The DCC shall provide dual instances of the order management system in resilient configuration across primary and secondary data centres.<br><br>All configurations & data are backed up with backups stored offsite. The DCC shall provide multiple network links & diverse routing. | The DCC shall do one or more of the following:<br><br>a) Capture orders using electronic or paper forms;<br>b) Restore the system from backups; and<br>c) On restoration of the system, the DCC shall ensure that all captured orders are entered. | Restoration of the CH Ordering System will not impact Incident Parties. | 1. In the event of a service interruption, Incident Parties shall submit orders as requested by the DCC.<br><br>2. No action is required from Incident Parties on restoration of the system. |

Table 4 – Business Continuity Procedures

## 6. Business Continuity and Disaster Recovery for Vodafone

6.1 The provisions of Section H10.13 shall not apply to the Services supported by the SMETS1 SM WAN for which Vodafone is the DCC Service Provider.

6.2 On the occurrence of a Disaster affecting the SMETS1 SM WAN for which Vodafone is the DCC Service Provider, the DCC shall take reasonable steps to restore any and all affected Services.

## 7. Planned Maintenance for Vodafone

7.1 The provisions of H8.4 shall not apply to Planned Maintenance of the SMETS1 SM WAN for which Vodafone is the DCC Service Provider.

7.2 Where Planned Maintenance is proposed to the SMETS1 SM WAN for which Vodafone is the DCC Service Provider, the DCC will provide 4 (four) Working Days' notice to Parties, to Registration Data Providers and to the Technical Architecture and Business Architecture Sub-Committee of the Planned Maintenance setting out the following information:

a) the proposed Maintenance activity (in reasonable detail);

b) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity;

c) the time and duration of the Maintenance activity; and

d) any associated risk that may subsequently affect the return of normal Services.