



Protecting the DCC Service User Policy- SEC H10

Version: 0.3

Date: 11.01.22

Owner: Ian Drummond (Director of Customer Relationship)

Author: Bilal Ali (Head of Customer Relationship)

Classification: DCC Controlled

Table of Contents

- 1. Introduction.....2
 - 1.1. Objective 2
 - 1.2. Scope 2
 - 1.2.1. Out of Scope 2
 - 1.3. Governance.....Error! Bookmark not defined.
- 2. Policy3
 - 2.1. Policy Statement..... 3
 - 2.2. Compliance 4
- 3. Responsibilities5
- 4. Definitions.....6
- 5. Related Documents.....6
- 6. Glossary6

1. Introduction

1.1. Objective

The DCC has an obligation to maintain service, as per SEC H.10, ensuring the DCC network is available at all times, for all Users, subject to maintenances, as per other critical national infrastructure networks.

Therefore, this policy sets out the tactical defensive actions DCC would undertake to protect the DCC network if the actions of a DCC User (or Users) were Compromising DCC network, or where there was an immediate threat of the DCC network being Compromised.

This policy describes how DCC would enact the allowance of user suspension detailed in SEC H10. Where the action of a User is considered to have caused the system to be compromised, that User (or Users) may be suspended, in whole or in part, from using DCC Services (for a limited timeframe), as a last resort.

For this Policy “Compromise” refers to a sub-section of the SEC definition and means:

in relation to any System, that the intended purpose or effective operation of that System is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity, or availability of the System or of any Data that are stored on or communicated by means of it

1.2. Scope

This Policy is applicable to all DCC Users and details what and when DCC would take action to protect the system from Compromise by instigating a partial or full suspension of DCC User. Suspension is only appropriate where a User’s actions are considered to be the cause of a DCC System Compromise and warnings have been unsuccessful in deterring actions to compromise.

This includes:

- Detailing the approach DCC will take in preventing and de-risking the network from any Compromise both proactively before any Compromise event occurs, and at the point Compromise occurs or where there is an immediate threat of Compromise.
- Detailing potential communication for Parties to de-risk the threat of Compromise over time.
- Detailing the communication / notification required where a User is suspended or partially suspended from the DCC Systems.

1.2.1. Out of Scope

This Policy is not applicable to:

- A security vulnerability or major security incident that results in partial or full suspension of a User’s activity
- Increasing DCC System capacity through any technical measures is not within the scope of this policy. This is let by CTO as part of the Continuity of Service workstream.
- Where any User’s actions are not considered to be the cause of DCC System Compromise.

1.3. Governance

The communication to key stakeholders during suspension activities will be led and managed by the Major Incident Management (MIM) Team. This will include:

- If a User is Suspended:
 - o MIM on shift manager will contact the User who has been/is being suspended via email and by phone, using the nominated contact list. During out of hours, MIM will email the User and follow up with a phone call during working hours.
 - o MIM on shift manager to inform SECAS within 24hr of suspending User, via email: SECAS@gemserv.com
 - Notification will include details of the scenario in which Compromise occurred or was imminent and how that was evaluated; details of engagement with the responsible Party to resolve the issue; and the length of the suspension.
 - If the suspension is ongoing at the point of Panel notification (due to significant risk) DCC will provide recommendations of User actions required before restoring service.
 - o MIM on shift manager to inform DCC Senior Stakeholders within 2 hr of User suspension, via the BAU MIM communication process.

MIM on shift manager will also open a bridge call with the wider suspension team (Technical Operations Centre (TOC), Communications Service Provider (CSP) & Service Ownership) when enacting suspension.

The policy is available to all employees on the DCC policy hub and will be available to all SEC Parties.

2. Policy (Enacting SEC H.10)

2.1. Policy Statement

DCC will protect the DCC network and look to manage the risk of Compromise by adhering to the following key principles:

- Users will be engaged by the service management team to help build forecasts of usage and usage trends
- DCC and Users should consider how to efficiently use the DCC network to proactively limit the threat of Compromise by sharing best practice on effective ways to maximise value from the DCC network
- Timely warning of thresholds or breaches will be communicated to the relevant User/s
- User Suspension should be a rare occurrence. DCC will not treat User suspension as BAU and will only be invoked as a last resort.
- Where suspension is deemed necessary, Technical Operations Centre (TOC) will monitor spikes in traffic against set thresholds across the DCC network and the DCC Major

Protecting the DCC Service User Policy- SEC H10

Incident Management Team will lead the process and have the authority and empowerment to suspend through appropriate control and decision points.

- Where suspension is deemed necessary, DCC will aim to partial suspend (specific Service Requests) rather than fully suspend a DCC User to reduce the impact to the User. There may be occasions where a full suspension of services is required.
- Where suspension has taken place, DCC will inform SEC Panel within 24 hours of the suspension taking place.
- DCC will manage the risk of Compromise by implementing the following stages:
 - Stage 0 Pre-emptive Engagement
 - Stage 1 Proactive engagement and triage of Risk to Service
 - Stage 2 Proactive Suspension as Part of Major Incident
 - Stage 3 – Reactive Suspension as Part of Major Incident
 - Stage 4 Removal of Suspension

The visual below demonstrates the triggers of each stage, the controls embedded, and the team empowered and accountable for each stage (a detailed Visio process is available if required):

	Stage 1 – Proactive Engagement	Stage 2 – Proactive Suspension	Stage 3 – Suspension/Major Incident	Post Suspension
Pre-emptive Engagement • All On-demand SR Users contacted • Other User demand forecasts obtained • Monthly service reviews with all key users • Challenge and share best practice on use of SRV's Responsible: • Customer Relationship Management Team (Retail and Non Retail)	Trigger: Rise in on-demand SRV's Vs forecast Likelihood of hitting lower threshold if trajectory continues.	Trigger: Thresholds reached, mitigation by user not successful. High risk of service disruption	Trigger: Incident that is linked to user on-demand traffic that is causing degradation or outage	Post Suspension • User engaged by MIM & Service Manager to agree plan to mitigate the issue going forward • Regular sessions diarised with User to assess the above • MIM to make decision on whether it's safe to resume the users service and if so, this will be implemented. If not, a get to green plan will be agreed with the user. • Updated comms issued to all key internal and external stakeholders
	Controls: - Fortnight review implemented with user to adjust utilisation through tactical recommendations or user system enhancements. - Share policy overview and impact of any compromise to the network - TOC to monitor customer usage trends - MIM to engage with the relevant Service Provider (SP) to confirm risk at cohort level	Outcome: Customer given warning DCC Suspends User (specific or all SRV's)	Outcome: DCC Suspends User (specific or all SRV's)	
	Responsible: - Customer Relationship Management - Major Incident Management Team	Controls: • Enhanced Monitoring from TOC • MIM to engage SP's to confirm risk of disruption and options available to de-risk • MIM log as Incident and set up Bridge Call with all key stakeholders • Where suspension is required, MIM Team Lead will be empowered to make the decision to suspend the user • Email sent to all key internal stakeholders • Email sent out to the user followed by a phone call from MIM to agree next steps • SECAS informed within 24hrs via email.	Controls: • Follows BAU MIM Process • For suspension, the same controls as the proactive suspension are followed.	
		Responsible: • MIM Team Leader/TOC Team Leader	Responsible: • MIM Team Leader/TOC	

- DCC will monitor and record frequency of all suspensions. Where reporting shows that suspension is becoming more common, DCC would look to understand the cause and what actions can be taken to reduce the likelihood of occurrence.

2.2. Compliance & Ownership of Policy

Monthly reporting will be undertaken to detail how system demand resulted in an early warning notice or breach of monitoring thresholds, and how many, if any, suspensions took place. These reports will be shared with the relevant key stakeholders and to SEC Panel at their request.

This reporting will be used to monitor the frequency of suspensions. The intention of this policy is that suspension is a rare occurrence. Where reporting shows that suspension is becoming more

common, DCC would look to understand the cause and what actions can be taken to reduce the likelihood of occurrence.

The Policy will be owned, maintained and the use and compliance of teams and individuals involved in the suspension process will be monitored by the Customer Relationship Management, Senior Incident Manager, Service Ownership and Capacity Management.

Exemptions

This policy may be exempt for certain Users who are involved in key industry activities, which occur on specific set a day's e.g., tariff updates at the start of each quarter due to changes in the price cap. This would be agreed, in advance, by the Director of Core Operations.

This Policy, however, does apply to Users not participating in these specific activities during those periods. TOC will continue to monitor the traffic from these Users during those key periods.

2.3. Out of Hours Working

As DCC operates a 24/7 service. Steps within this policy may need to be enacted outside of normal working hours. DCC MIM lead will engage with a User, as described in the above stages, but it is expected that a User will not be able to fully respond until the next working day.

DCC will continue to monitor System usage and, if possible, cease the suspension where other traffic would allow that to happen without the risk of Compromise to DCC Systems.

If a User is suspended out of hours and system usage shows that is not possible to cease suspension without continuing the risk of Compromise to DCC Systems, then suspension will likely need to remain in place until User has been in contact with DCC and remedial actions have been agreed.

During out of hours, the TOC (being the 24/7 team) will carry out the following steps ahead of handing over to the MIM team, who, if required, will follow the process to suspend the customer if absolutely needed:

1. Investigate the increased volumes and trigger of any threshold alerts
2. Confirm whether it was from one SU or multiple parties
3. Confirm whether there is any degradation of SRVs (or service) caused by the influx/spikes of traffic (whether it be categories 1, 2 or 3 level)
4. If investigation confirms degradation of service TOC will then engage MIM to take the necessary actions.

3. Policy Responsibilities

Responsible:		Accountable:	
- Technical Operations Centre Lead - Major Incident Management Team Lead		Director of Customer Relationship Management	
Consulted:		Informed:	

- DCC User
- DCC Service Provider
- DCC Customer Relationship Management
- DCC Regulations
- DCC Security
- SEC Panel - SECAS@gemserv.com
- Key DCC Senior Stakeholders

4. Definitions

Acronym	Definition
BAU	Business as usual
DCC	Data Communication Company
SEC	Smart Energy Code
SR	Service Request

5. Related Documents

- Incident Management Policy
- Section H.10 of SEC
- System Monitoring and Enactment of User Suspension Process includes templates for communications

6. Glossary

Term	Definition
Partial Suspension	a reduction of any DCC Service
Proactive Suspension	a Suspension or partial Suspension implemented before system Compromise has occurs
Suspension	complete removal of DCC Services
Threshold	The volume of demand at any point of the DCC System that triggers an early warning of high demand