

Network Incidents

Users' Guide for the Incident Reporting Portal on Data.ComReg

Information Notice

Reference: ComReg 24/41R1

Version: Final

Date: 03/10/2025

Additional Information

Document No:	ComReg 24/41R1
Date:	03/10/2025

Content

- 1: Introduction..... 4
 - 1.1 Background..... 4
 - 1.2 Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 4
 - 1.3 Reporting Portal and Changes to the Users’ Guide 5
 - 1.4 Structure of this document 6
- 2: Account Creation and Logging In 7
- 3: Reporting Security Incidents 13
 - 3.1 Report a new Security Incident 13
 - 3.2 Update a security Incident Report..... 17
 - 3.3 Closing a security Incident Report 21
- 4: Reporting Storm Incidents..... 25
 - 4.1 Report new Storm Incident..... 25
 - 4.2 Update Storm Incident Report..... 31
 - 4.3 Close Storm Incident Report..... 33

1: Introduction

1.1 Background

The Commission for Communications Regulation (“ComReg”) is the statutory body responsible for the regulation of the electronic communications (telecommunications, radiocommunication and broadcasting networks), postal and premium rate sectors in Ireland in accordance with European Union (“EU”) and Irish law. ComReg also manages Ireland’s radio spectrum (or “spectrum”) and national numbering resource¹.

The online portal for the reporting of security incidents (“Portal”) was introduced in 2019 to facilitate incident reporting while the data required by it for reporting largely continued to be that set out in the previous Incident Reporting Form 14/02a². The Portal not only enabled the online reporting of a new incident but also facilitated the updating of information in relation to incidents in progress. Security features of the Portal includes two-factor authentication, with only registered users and their authorised representatives having access to the portal. In December 2022, ComReg added the reporting of ‘Storm’ Incidents.

1.2 Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023

In 2023, following the transposition of the European Electronic Communications Code (“EECC”) by the Communications Regulation and Digital Hub Development Agency (Amendment) Act of 2023, Act No. 4 of 2023 (the “Act of 2023”), ComReg published a consultation³ introducing changes to the framework for the reporting of security incidents⁴

¹ ComReg Doc 21/136 – <https://www.comreg.ie/publication/radio-spectrum-management-strategy-statement-2022-to-2024-designed-version-comreg-21-136>

² ComReg Incident Reporting Template – <https://www.comreg.ie/publication/comreg-incident-reporting-template/>

³ Network Incident Reporting Thresholds, A consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards) – ComReg Document 23/36 – <https://www.comreg.ie/media/2023/04/ComReg-2336-2.pdf>.

⁴ Security incidents, as defined in section 5 of the Act of 2023, and henceforth “Incidents” and security incidents are used interchangeably in both this document and in the Portal.

("incidents"). Subsequently, in 2024, ComReg published a Response to Consultation and an associated Decision Instrument⁵.

1.3 Reporting Portal and Changes to the Users' Guide

Following the publication of ComReg Document 24/23 and its Decision Instrument D08/24, the Portal was updated for consistency with these documents, and the following functions were added:

- the selection of a security incident type ('Storm', 'Isolated' and 'Malicious');
- the selection of a security incident sub-category;
- reporting for security Incidents affecting Number Independent Interpersonal Communication Service ("NI-ICS") providers; and
- updating the service and network asset types to reflect those used in the provision of modern networks and services.

Consequently, in 2024, ComReg replaced the user guidance (ComReg 19/98⁶), with an updated guidance (ComReg 24/41⁷) for the Portal for reporting security incidents affecting providers of ECN, ECS and NI-ICS.

In 2025, ComReg migrated the incident reporting portal to Data.ComReg.ie Platform ("Data.ComReg"). As part of the Data.ComReg each user will have their own personal login set up to be able to access their organisation's account they are associated with.

This document, ComReg 24/41R1, is the user's guide for using the incident reporting Portal on Data.ComReg (<https://data.comreg.ie/>) for reporting security incidents affecting providers of ECN, ECS and NI-ICS and revises ComReg 24/41⁷.

⁵ Network Incident Reporting Thresholds: Response to Consultation, On the revision and replacement of ComReg Document 14/02 (Reporting & Guidance on Incident Reporting Minimum-Security Standards) - ComReg Document 24/23 – <https://www.comreg.ie/publication/network-incident-reporting-thresholds-response-to-consultation>

⁶ User Guide for ComReg's Network Incident Reporting portal – <https://www.comreg.ie/publication/user-guide-for-comregs-network-incident-reporting-portal>

⁷ User Guide for ComReg's e-licensing Network Incident Reporting portal [ComReg-2441.pdf](#)

While this document structure is similar to its predecessor, it has been updated with new screen captures, which reflect the new user interface of the Data.ComReg, and the login steps to access it.

1.4 Structure of this document

This document is structured as follow:

- Section 2 (Account Activation and First Login), provides the steps to register, activate an account, and login for the first time;
- Section 3 (Reporting security Incidents), provides the steps to create, update, and close a security incident under Isolated and Malicious types; and
- Section 4 (Reporting Storm Incidents), provides the steps to create, update, and close a storm incident.

In order to clarify for the user when using this guide, the page names and the button⁸ functions to press are indicated as below:

- ***Italic and Bold*** font, indicates the page's name – i.e., ***Network Incident Reporting – Incident list*** page.
- "Inverted Comma" and underlined font, indicates the button's function (press button) – i.e. click on "New incident".

In case of issues using the incident reporting Portal on Data.ComReg, and for further clarifications, ComReg can be contacted via the following dedicated email (incident@comreg.ie).

⁸ All functionality is accessed by clicking on tagged buttons on each part of the form. The guide takes the operator through the steps, including buttons to press, to report an incident.

2: Account Creation and Logging In

When registering to use the incident reporting Portal on Data.ComReg as a new user⁹, ComReg will request users to provide at least one contact who is tasked with submitting security incidents to the Portal. In order to complete the registration and the account setup to become a user, the following information needs to be supplied via the dedicated email (incident@comreg.ie).

- Company Name;
- Office Address;
- Name of Contact Person(s);
- Contact Number; and
- Email Address.

⁹ Existing users: do not need to re-register to use Data.ComReg Portal. However, when using the Data.ComReg Portal for the first time, they will need to set up their log in.

After ComReg creates the account, an email will be sent to the contact person(s) advising them of the account creation and with instructions as to how to activate the account. A screenshot of the email template is shown below:

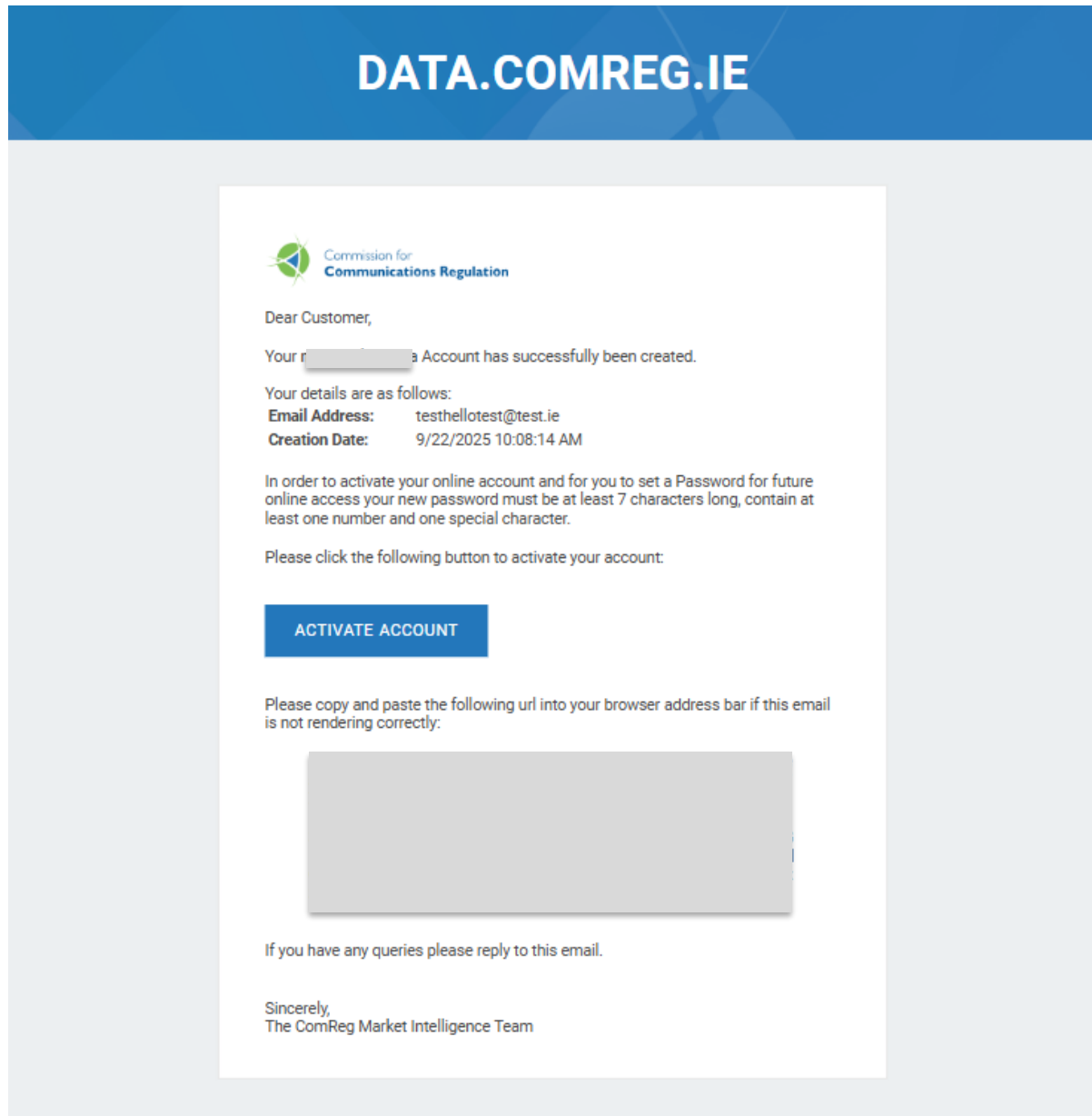


Figure 1: Email Confirming Account Creation

Clicking on the “Activate Account” function (Figure 1 above), will redirect the user to the **Set New Password** page. The user will be asked to create a personal password that is a minimum of 7 characters long, containing at least one number and one special character. The user can then click on “SET NEW PASSWORD”. A screenshot of the **Set New Password** page is shown in Figure 2 below.

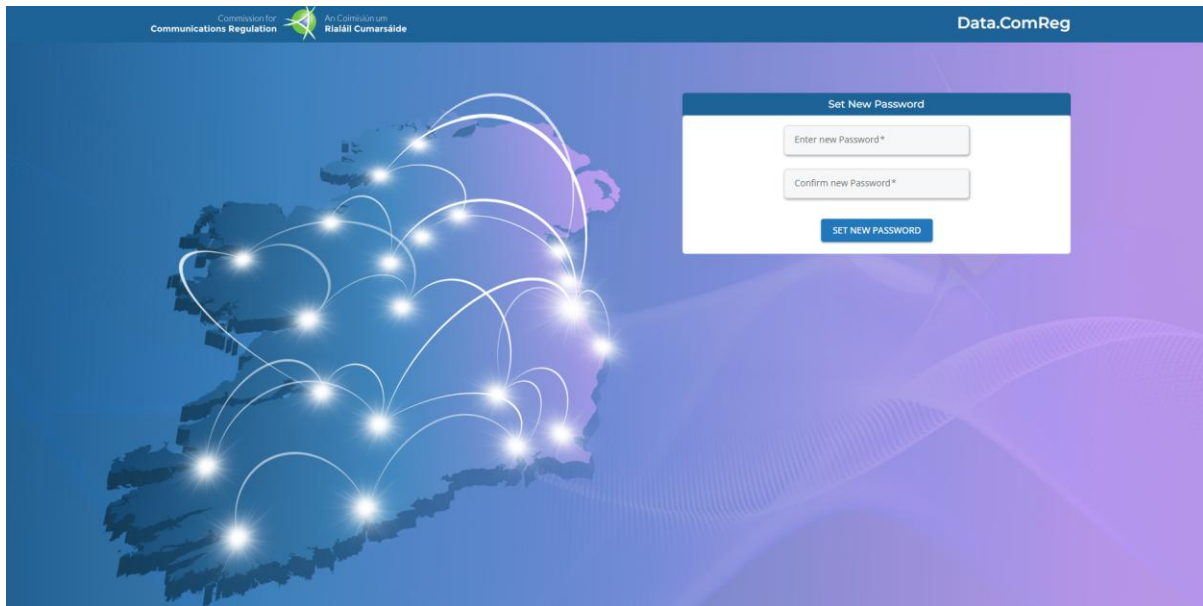


Figure 2: Set New Password Page

After setting the password successfully, a confirmation page will appear, as shown in Figure 3 below, the user can click on “[Return to Log In](#)”.

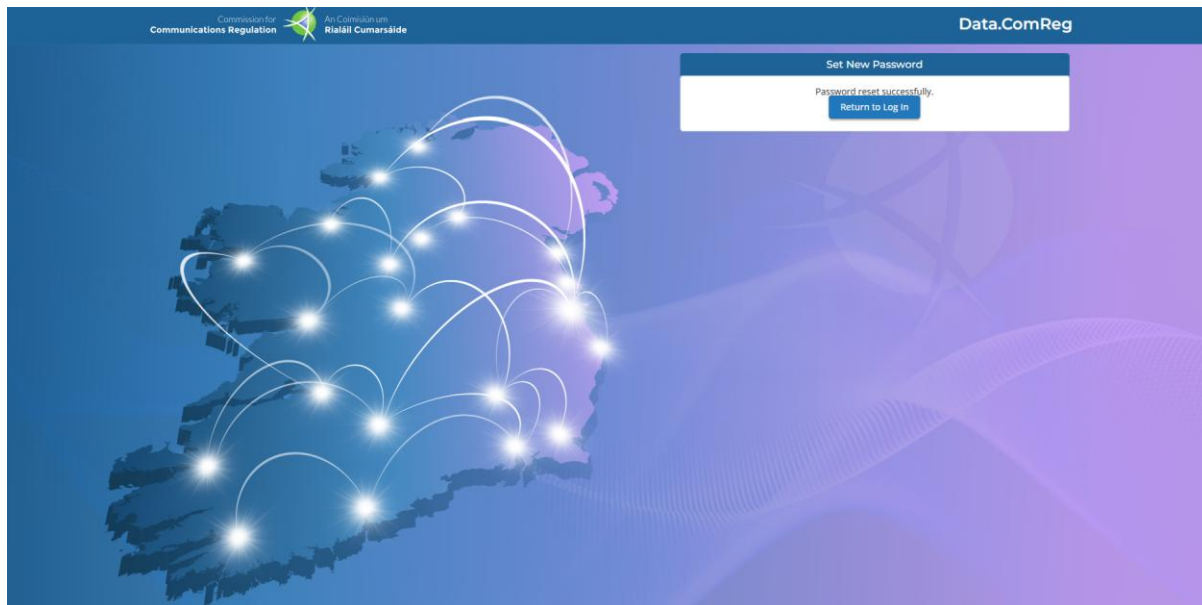


Figure 3: Successful Password Set up Confirmation

The user can now login to the Data.ComReg. The user will be asked to provide the “Email Address” and “Password”, then click on “[Log In](#)”. Figure 4 below shows a screenshot of this page.

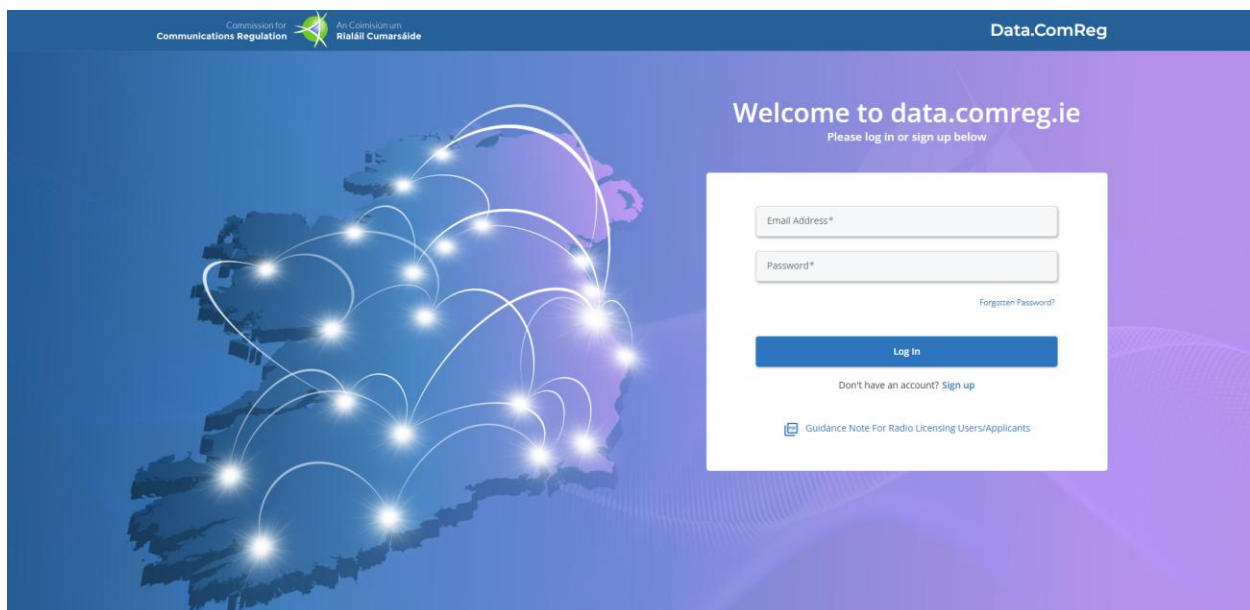


Figure 4: logging in Page

After clicking on the “Log in” function, the user will be asked to set up Multi-Factor Authentication (MFA/2FA). When logging in for the first time¹⁰, users will be prompted to set up Multi-Factor Authentication:

- A QR code will be displayed for scanning with an authenticator app of their choice
- Alternatively, a manual code will be provided if the QR code cannot be scanned.

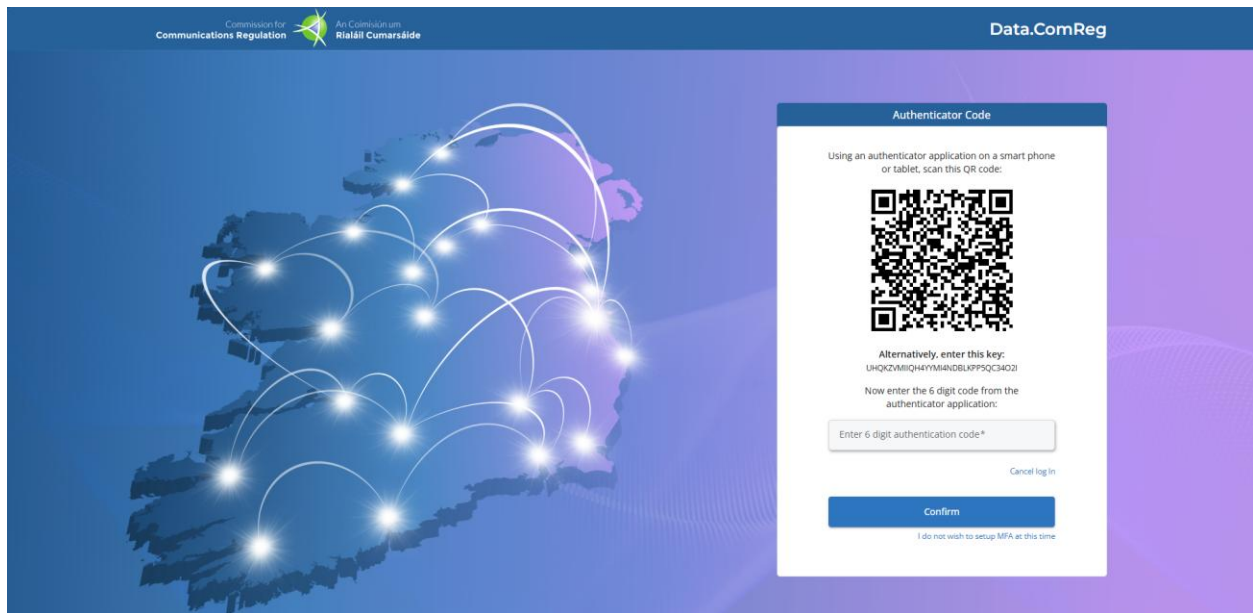


Figure 5: Authenticator Code Page

¹⁰ This step is only required for the first time that a user is setting up their log in.

As part of two-factor authentication, the user will then be asked to input the 6-digit authentication code, which will be generated by the user's authentication app, then click on "Confirm", as shown in Figure 6 below.

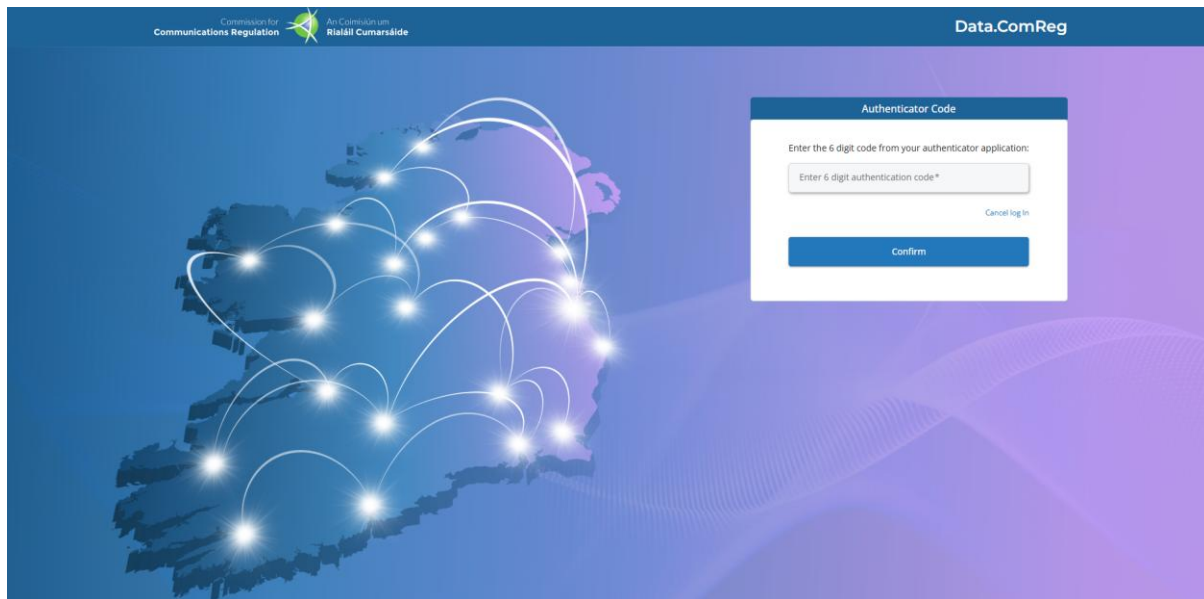


Figure 6: Logging in – Authentication Code

The user is now routed to the **Network Incident Reporting** page.

3: Reporting Security Incidents¹¹

After logging in, the user will be routed to the **Network Incident Reporting – Incident list** page, which provides the option to report a new security incident and also lists the security incidents that have already been created.

3.1 Report a new Security Incident

In order, to create a new security incident report, click on “New incident” as shown in Figure 7 below.

Commission for Communications Regulation / An Coimisiún um Rialáil Cumarsáide

Data.ComReg

NOUTestAccount

Click on “New incident”

Network Incident Reporting - Incident list

Search Incidents: [Show All](#) [Help / Instructions](#) [New Incident](#)

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Action
125996-NO000204	12/05/2025, 00:00	12/05/2025, 01:00	da	Closed	Mark Kane	
125996-NO000203	11/05/2025, 02:00	11/05/2025, 03:30	HLR Down	Closed	Mark Kane	
125996-NO000208	11/06/2025, 00:30	11/06/2025, 02:00	Iso to Mali	Closed	Ihab Zine	
125996-NO000207	11/06/2025, 00:30	11/06/2025, 01:00	Malicious test 11 June 25	Closed	Ihab Zine	
125996-NO000206	11/06/2025, 00:00	11/06/2025, 04:00	Storm Test 11 June 25	Closed	Ihab Zine	
125996-NO000205	11/06/2025, 00:00	11/06/2025, 01:00	Test 11 June 25	Closed	Ihab Zine	
125996-NO000202	07/05/2025, 06:30		Test Type Change	Open	Darren Nulty	Update
125996-NO000201	30/04/2025, 06:00	30/04/2025, 06:30	Test Incident	Closed	Darren Nulty	
125996-NO000200	23/04/2025, 02:00	24/04/2025, 04:00	drag	Closed	Mark Kane	
125996-NO000199	15/04/2025, 00:30	15/04/2025, 01:00	test	Closed	Ihab Zine	

Items per page: 10 1 - 10 of 20

For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.

Figure 7: Network Incident Reporting – Incident list Page

¹¹ This section provides guidance for reporting security incidents under the Isolated or Malicious types. The process and template are the same for reporting such security incidents. The difference is in some of the required information which is relevant to each security incident type.

Next, the user will be routed to the **Create Incident Report** page, as shown in Figure 8 below. In this page the user is required to do the following:

- 1) Select the security incident type (Isolated, Storm, or Malicious¹²)
- 2) Select the affected sub-category (Authenticity, Availability, Confidentiality, or Integrity), note that more than one sub-category may be affected.
- 3) Provide the relevant summary information: Title, Date and Time, and Description of the incident;
- 4) Tick the boxes of the services affected; under Fixed Services, Mobile Services (both) and/or NI-ICS Services, where appropriate; and
- 5) Click on “Create Incident” when the required information has been provided.

The screenshot shows the 'Create Incident Report' page. At the top, there is a blue header bar with the text 'Create Incident Report'. Below this, there are two buttons: 'Expand All' and 'Collapse All'. The main form is divided into sections. The first section is 'Summary', which contains the 'Incident Type' section with three radio buttons: 'Isolated' (selected), 'Storm', and 'Malicious'. Below this is a 'Title*' text input field. The next section is 'Start Date and Time of Incident', which includes a 'Select or Enter Time*' dropdown and a 'Date' input field with a calendar icon. Below this is the 'Sub Categories' section with four checkboxes: 'Authenticity', 'Availability', 'Confidentiality', and 'Integrity'. A large text area for 'Description of Incident*' follows. At the bottom, there are three sections for services: 'Fixed Services', 'Mobile Services', and 'NI-ICS', each with a dropdown arrow. At the very bottom, there are two buttons: 'Back' and 'Create incident'. Numbered callouts are placed over the form: '1' points to the 'Incident Type' section, '2' points to the 'Sub Categories' section, '3' points to the 'Title*' field, the 'Date' field, and the 'Description of Incident*' text area, '4' points to the service dropdowns, and '5' points to the 'Create incident' button.

Figure 8: Create Incident Report Page

¹² This type of security incident is intended to catch those that include but are not limited to those caused by the malicious actions of a third party, whether of a cyber or other origin (i.e., arson, physical damage etc.).

Note that when the user ticks the “Yes” box for Fixed Services, Mobile Services, and/or NI-ICS, the user will be required to select if the security incident has impacted the Service Offering(s) for Retail or Wholesale. In addition, the user will be required to provide further information on the Number of End Users Affected and Quantity of Sites Affected¹³, as shown in Figure 9 below.

The screenshot displays the 'Create Incident Report' form. At the top, there's a blue header bar with the title 'Create Incident Report' and two buttons: 'Expand All' and 'Collapse All'. Below this is a 'Summary' section with a blue header. It contains several fields: 'Incident Type' with radio buttons for 'Isolated' (selected), 'Storm', and 'Malicious'; a 'Title' field with the value 'Incident Report Test'; 'Start Date and Time of Incident' with a time field set to '12:00' and a date field set to '08/09/2025'; 'Sub Categories' with checkboxes for 'Authenticity' (checked), 'Availability' (checked), 'Confidentiality' (unchecked), and 'Integrity' (unchecked); and a 'Description of Incident' field with the text 'This Incident is created for the purpose of demonstration.' and a summary line 'Selected Type: Isolated. Selected sub-category: Authenticity and Availability'. Below the 'Summary' section is the 'Fixed Services' section, which is expanded. It contains 'Mobile Services' and 'NI-ICS'. Under 'Mobile Services', there are sections for 'ECAS' (Yes/No, with 'No' selected), 'Data Service' (Yes/No, with 'Yes' selected), and 'Service Offering(s) Affected'. Under 'Service Offering(s) Affected', 'Retail' is checked, and there are input fields for 'Number of End Users Affected' (0) and 'Quantity of Sites Affected' (0). There is also an unchecked 'Wholesale' option. Below 'Mobile Services' is the 'Voice Service' section with Yes/No radio buttons (No is selected). At the bottom of the form are 'Back' and 'Create Incident' buttons.

Figure 9: Example of the Create Incident Report Page with Mobile Services Affected

¹³ In the case of the Fixed Service or NI-ICS this includes but is not limited to: Points of Presence, Data centres, Interconnect points etc.

After Steps 1 to 5 above have been completed and the function “Create Report” has been clicked, a pop-up window called ***Incident Created*** will appear, giving the user two options, “Update Incident Report now”, or “Update Incident Report later” – this is shown in Figure 10 below.

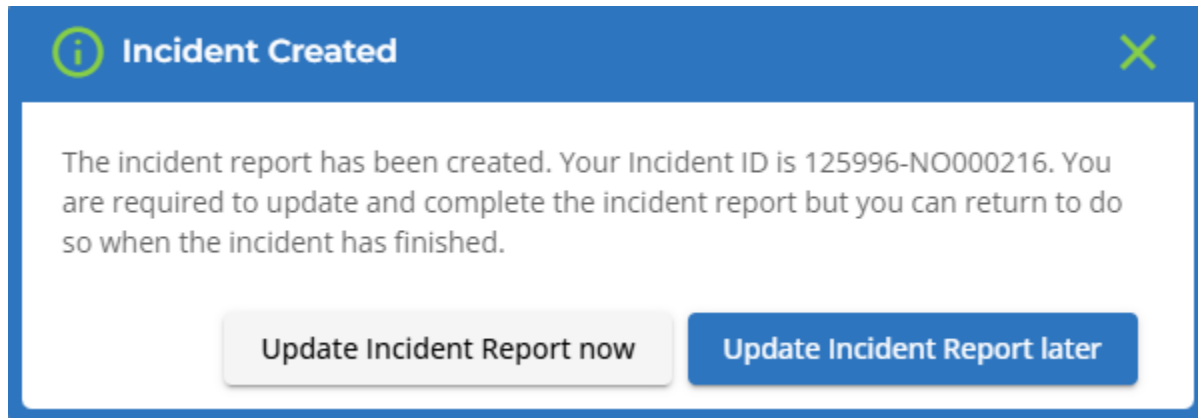


Figure 10: Incident Created Pop-Up Window

Sub-Section 3.2 below, provides the steps that are required to update an existing security incident report.

3.2 Update a security Incident Report

The user is required to update the submitted information while a security incident remains open and to complete the report.

An existing security incident report can be updated by logging into the **Network Incident Reporting – Incident list** page. The report to be updated can be chosen from the Incident list. Note that, only open security incidents in the list will have the update button available, and therefore, can be updated.

The required steps to update a report are as follows:

- 1) As shown in Figure 11 below, click on “Update”;

Commission for Communications Regulation An Coimisiún um Rialáil Cumarsáide

Data.ComReg

NOUTestAccount

1

Network Incident Reporting – Incident list

Search Incidents: Show All Help / Instructions New Incident

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Action
125996-NO000216	08/09/2025, 12:00		Incident Report Test	Open	Ihab Zine	Update
125996-NO000204	12/05/2025, 00:00	12/05/2025, 01:00	da	Closed	Mark Kane	
125996-NO000203	11/05/2025, 02:00	11/05/2025, 03:30	HLR Down	Closed	Mark Kane	
125996-NO000208	11/06/2025, 00:30	11/06/2025, 02:00	Iso to Mali	Closed	Ihab Zine	
125996-NO000207	11/06/2025, 00:30	11/06/2025, 01:00	Malicious test 11 June 25	Closed	Ihab Zine	
125996-NO000206	11/06/2025, 00:00	11/06/2025, 04:00	Storm Test 11 June 25	Closed	Ihab Zine	
125996-NO000205	11/06/2025, 00:00	11/06/2025, 01:00	Test 11June25	Closed	Ihab Zine	
125996-NO000202	07/05/2025, 06:30		Test Type Change	Open	Darren Nulty	Update
125996-NO000201	30/04/2025, 06:00	30/04/2025, 06:30	Test Incident	Closed	Darren Nulty	
125996-NO000200	23/04/2025, 02:00	24/04/2025, 04:00	drag	Closed	Mark Kane	

Items per page: 10 1 – 10 of 21

For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.

Figure 11: Network Incident Reporting Page – Incident list

- 2) Next, in the **Update Incident Report** page – Figure 12 and Figure 13 – provide the required information. Then, click on “Save Changes”; and
- 3) If the security incident is still open, and the user wishes to exit from the **Update Incident Report** page, click on “Home Icon” function. The user will be routed back to the **Network Incident Reporting – Incident list** page.

Figure 12: Update Incident Report Page

☒ Yes ☐ No

Service Offering(s) Affected

☒ Retail

Number of End Users Affected
 1 ⓘ

Quantity of Sites Affected
 1 ⓘ

☐ Wholesale

Platform(s) Affected

<input type="checkbox"/> Copper Access ⓘ	<input type="checkbox"/> Copper Backhaul ⓘ
<input type="checkbox"/> Fibre Access ⓘ	<input type="checkbox"/> Fibre Backhaul
<input type="checkbox"/> SIP	<input type="checkbox"/> GSM
<input type="checkbox"/> UMTS	<input type="checkbox"/> LTE
<input type="checkbox"/> LTE+	<input type="checkbox"/> Radio Access
<input type="checkbox"/> Radio Backhaul	<input type="checkbox"/> VoIP/VoLTE
<input type="checkbox"/> 5G Stand-Alone Radio	<input type="checkbox"/> 5G New Radio (NR)
<input type="checkbox"/> 5G Non-Stand-Alone (NSA)	<input type="checkbox"/> Other

Assets(s) Affected

<input type="checkbox"/> Authentication	<input type="checkbox"/> Backhaul
<input type="checkbox"/> Base Stations ⓘ	<input type="checkbox"/> Billing/Operational Support System
<input type="checkbox"/> Copper ⓘ	<input type="checkbox"/> Core
<input type="checkbox"/> DNS	<input type="checkbox"/> DSLAM
<input type="checkbox"/> Fibre	<input type="checkbox"/> Firewall
<input type="checkbox"/> Gateway	<input type="checkbox"/> Interconnect
<input type="checkbox"/> Network Control ⓘ	<input type="checkbox"/> Radio
<input type="checkbox"/> Router	<input type="checkbox"/> Server
<input type="checkbox"/> Signalling SS7	<input type="checkbox"/> Signalling Diameter
<input type="checkbox"/> Signalling Radius	<input type="checkbox"/> Signalling Other
<input type="checkbox"/> SIP	<input type="checkbox"/> Switch
<input type="checkbox"/> VoIP/VoLTENode	<input type="checkbox"/> Wholesale Services
<input type="checkbox"/> Authorisation	<input type="checkbox"/> Charging (PRCF)
<input type="checkbox"/> Policy Rules	<input type="checkbox"/> Slicing
<input type="checkbox"/> Virtualised Network	<input type="checkbox"/> Other

Root Causes

<input type="checkbox"/> Cooling Failure	<input type="checkbox"/> Malicious Actions ⓘ
<input type="checkbox"/> Natural Phenomena ⓘ	<input type="checkbox"/> Power Failure
<input type="checkbox"/> System Failure ⓘ	<input type="checkbox"/> Third Party Failure
<input type="checkbox"/> Other	

Selecting this will change the Incident Type to "Malicious" and remove any other Root Causes selected when you Save or Close this incident.

Voice Service

☐ Yes ☒ No

NI-ICS

Figure 13: Update Incident Report Page

If the security incident has ended, and the Root Cause Analysis (“RCA”) has been satisfactorily completed by the user concerned, to ComReg’s satisfaction, the user can then follow the required steps in sub-section 3.3 below, to close the security incident report.

3.3 Closing a security Incident Report

As the security incident has ended, and the root cause analysis has been satisfactorily completed by the user concerned to ComReg's satisfaction, the report can be closed as follows:

- 1) Click on "Save Changes"; then
- 2) click on "Close Incident" as shown in Figure 14 below.

☒ Yes ☐ No

Service Offering(s) Affected

☒ Retail

Number of End Users Affected: 1

Quantity of Sites Affected: 1

☐ Wholesale

Platform(s) Affected

<input type="checkbox"/> Copper Access	<input type="checkbox"/> Copper Backhaul
<input type="checkbox"/> Fibre Access	<input type="checkbox"/> Fibre Backhaul
<input type="checkbox"/> SIP	<input type="checkbox"/> GSM
<input type="checkbox"/> UMTS	<input type="checkbox"/> LTE
<input type="checkbox"/> LTE+	<input type="checkbox"/> Radio Access
<input type="checkbox"/> Radio Backhaul	<input type="checkbox"/> VoIP/VoLTE
<input type="checkbox"/> 5G Stand-Alone Radio	<input type="checkbox"/> 5G New Radio (NR)
<input type="checkbox"/> 5G Non-Stand-Alone (NSA)	<input type="checkbox"/> Other

Assets(s) Affected

<input type="checkbox"/> Authentication	<input type="checkbox"/> Backhaul
<input type="checkbox"/> Base Stations	<input type="checkbox"/> Billing/Operational Support System
<input type="checkbox"/> Copper	<input type="checkbox"/> Core
<input type="checkbox"/> DNS	<input type="checkbox"/> DSLAM
<input type="checkbox"/> Fibre	<input type="checkbox"/> Firewall
<input type="checkbox"/> Gateway	<input type="checkbox"/> Interconnect
<input type="checkbox"/> Network Control	<input type="checkbox"/> Radio
<input type="checkbox"/> Router	<input type="checkbox"/> Server
<input type="checkbox"/> Signalling SS7	<input type="checkbox"/> Signalling Diameter
<input type="checkbox"/> Signalling Radius	<input type="checkbox"/> Signalling Other
<input type="checkbox"/> SIP	<input type="checkbox"/> Switch
<input type="checkbox"/> VoIP/VoLTENode	<input type="checkbox"/> Wholesale Services
<input type="checkbox"/> Authorisation	<input type="checkbox"/> Charging (PCRF)
<input type="checkbox"/> Policy Rules	<input type="checkbox"/> Slicing
<input type="checkbox"/> Virtualised Network	<input type="checkbox"/> Other

Root Causes

<input type="checkbox"/> Cooling Failure	<input type="checkbox"/> Malicious Actions
<input type="checkbox"/> Natural Phenomena	<input type="checkbox"/> Power Failure
<input type="checkbox"/> System Failure	<input type="checkbox"/> Third Party Failure
<input type="checkbox"/> Other	

Selecting this will change the incident type to "Malicious" and remove any other Root Causes selected when you Save or Close this incident.

Voice Service

☐ Yes ☒ No

NI-ICS

Figure 14: Update Incident Report Page

A pop-up window called ***Incident Closed*** will appear to confirm that the incident has been closed successfully as shown in Figure 15 below.

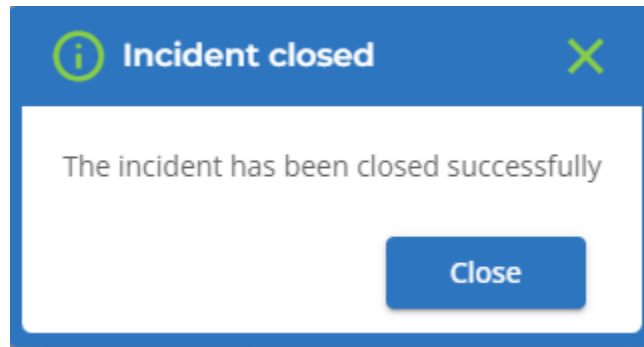


Figure 15: Incident Closed Pop-Up Window

Once the security incident report has been closed, the update function will be deactivated and the status of the report will be indicated as closed, as shown in Figure 16 below.

Commission for Communications Regulation An Coimisiún um Rialáil Cumarsáide





Data.ComReg

Home A/C 125996

NOUTestAccount

Network Incident Reporting - Incident list

Search Incidents: [Show All](#) [Help / Instructions](#) [New incident](#)

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Action
125996-NO000216	08/09/2025, 12:00	08/09/2025, 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000204	12/05/2025, 00:00	12/05/2025, 01:00	da	Closed	Mark Kane	
125996-NO000203	11/05/2025, 02:00	11/05/2025, 03:30	HLR Down	Closed	Mark Kane	
125996-NO000208	11/06/2025, 00:30	11/06/2025, 02:00	Iso to Mali	 Closed	Ihab Zine	
125996-NO000207	11/06/2025, 00:30	11/06/2025, 01:00	Malicious test 11 June 25	 Closed	Ihab Zine	
125996-NO000206	11/06/2025, 00:00	11/06/2025, 04:00	Storm Test 11 June 25	 Closed	Ihab Zine	
125996-NO000205	11/06/2025, 00:00	11/06/2025, 01:00	Test 11June25	Closed	Ihab Zine	
125996-NO000202	07/05/2025, 06:30		Test Type Change	Open	Darren Nulty	Update
125996-NO000201	30/04/2025, 06:00	30/04/2025, 06:30	Test Incident	Closed	Darren Nulty	
125996-NO000200	23/04/2025, 02:00	24/04/2025, 04:00	drag	 Closed	Mark Kane	

Items per page: 1 - 10 of 21

For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.

Figure 16: Network Incident Reporting – Incident list Page with a Closed Incident

Note that, as the security incident report has been closed, it will not be possible to open the report or make any further changes. Should it be required by the user, ComReg, in exceptional circumstances and at its sole discretion, may reopen the report, to allow the user to make any corrections or to submit further information.

Note also that, if the user fails to close out the security Incident report within 30 calendar days, an email will be sent reminding them to do so. This ensures that cases are closed, once root cause analysis is completed.

4: Reporting Storm Incidents

To allow for a simplified storm reporting, operators **must** report storm incidents via the incident reporting Portal.

When Met Éireann indicates that a named storm or weather event is expected and that Orange or Red Level warnings¹⁴ are to be in operation; ComReg will e-mail registered operators notifying them that reports on the condition of their networks and services will be required. The deadlines for reporting the impact of the storm on registered Operators' networks and services will remain the same; at the times of 10H00 and 16H00.

4.1 Report new Storm Incident

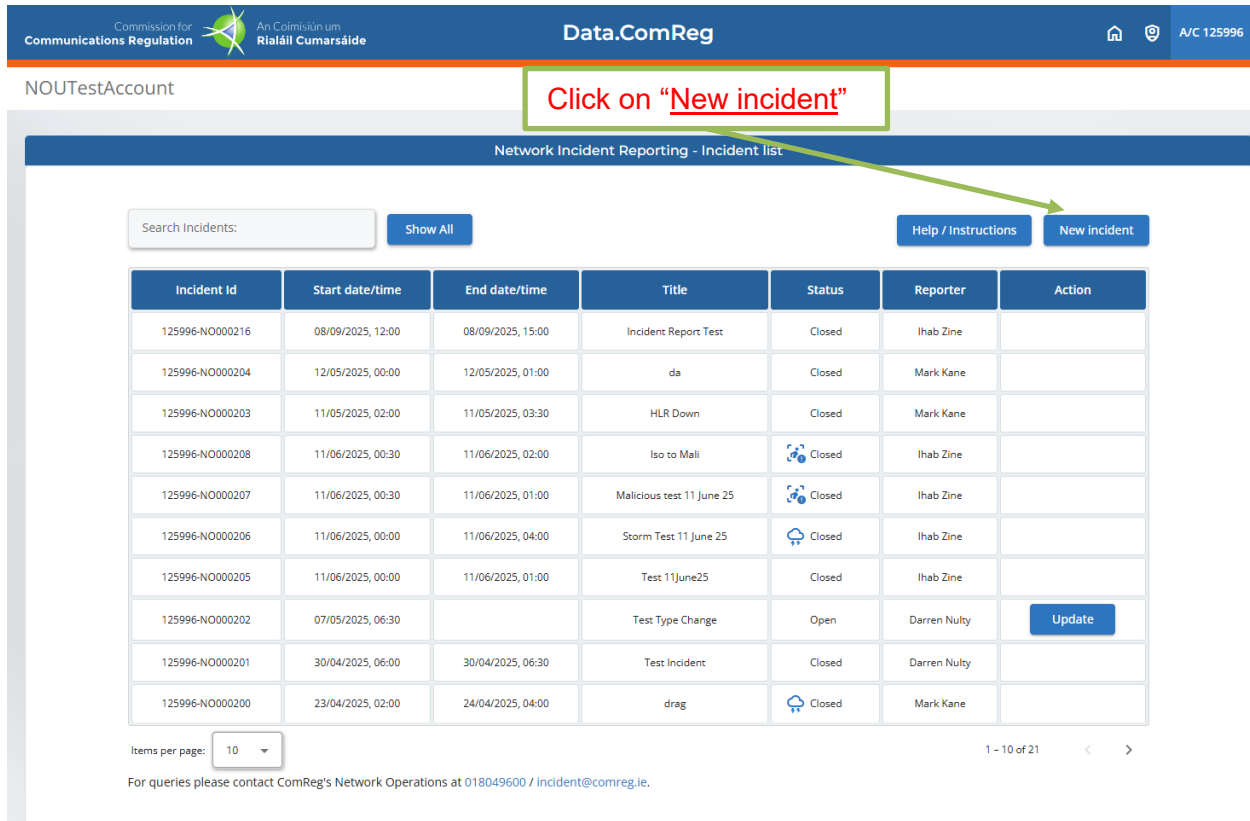
After logging in to the Data.ComReg (<https://data.comreg.ie/>) – as shown by 4 to Figure 7 in section 2 above – the user will be routed to the **Network Incident Reporting – Incident list** page, which provides the option to report a new incident.

¹⁴ Met Éireann uses and issues different warning levels (Yellow, Orange, Red) depending on the expected severity of the weather event. The warning levels are defined as follows:

- Yellow: Weather that does not pose a threat to the general population but is potentially dangerous on a localised scale.
- Orange: Infrequent and dangerous weather conditions which may pose a threat to life and property.
- Red: Rare and very dangerous weather conditions from intense meteorological phenomena.

For more details see: [Weather warnings explanation - Met Éireann - The Irish Meteorological Service](#)

In order, to create a new storm report, click on “New incident” as shown in Figure 17 below.







Commission for Communications Regulation An Coimisiún um Rialáil Cumarsáide Data.ComReg A/C 125996

NOUtestAccount

Click on “New incident”

Network Incident Reporting - Incident list

Search Incidents: Show All Help / Instructions New incident

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Action
125996-NO000216	08/09/2025, 12:00	08/09/2025, 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000204	12/05/2025, 00:00	12/05/2025, 01:00	da	Closed	Mark Kane	
125996-NO000203	11/05/2025, 02:00	11/05/2025, 03:30	HLR Down	Closed	Mark Kane	
125996-NO000208	11/06/2025, 00:30	11/06/2025, 02:00	Iso to Mali	 Closed	Ihab Zine	
125996-NO000207	11/06/2025, 00:30	11/06/2025, 01:00	Malicious test 11 June 25	 Closed	Ihab Zine	
125996-NO000206	11/06/2025, 00:00	11/06/2025, 04:00	Storm Test 11 June 25	 Closed	Ihab Zine	
125996-NO000205	11/06/2025, 00:00	11/06/2025, 01:00	Test 11June25	Closed	Ihab Zine	
125996-NO000202	07/05/2025, 06:30		Test Type Change	Open	Darren Nulty	<input type="button" value="Update"/>
125996-NO000201	30/04/2025, 06:00	30/04/2025, 06:30	Test Incident	Closed	Darren Nulty	
125996-NO000200	23/04/2025, 02:00	24/04/2025, 04:00	drag	 Closed	Mark Kane	

Items per page: 10 1 - 10 of 21

For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.

Figure 17: Create Storm Report from Network Incident Reporting – Incident list Page

Next, the user will be routed to the **Create Incident Report** page, as shown in Figure 18 below. In this page the user is required to do the following:

- 1) Tick the box for “Storm”, as shown below;
- 2) Provide the relevant summary information Title (Name of the Storm), Date and Time, and Description of incident;

The screenshot shows the 'Create Incident Report' form. At the top is a blue header bar with the text 'Create Incident Report'. Below this is a 'Summary' section with a blue header and an expand/collapse toggle. The 'Incident Type' section has three radio buttons: 'Isolated', 'Storm' (which is selected), and 'Malicious'. A green box with the number '1' is around the 'Storm' radio button, with an arrow pointing to it. The 'Title:*' field is a text input. The 'Start Date and Time of Incident:' section has a 'Select or Enter Time*' dropdown and a 'Date' field with a calendar icon. A green box with the number '2' is around the 'Date' field, with arrows pointing to it from the 'Title' field and the 'Description of Incident*' field. The 'Sub Categories:' section has four checkboxes: 'Authenticity', 'Availability', 'Confidentiality', and 'Integrity'. The 'Description of Incident*' field is a large text area. Below this is a 'Services Affected' section with a blue header and a dropdown arrow. It contains four items: 'Fixed Services', 'Mobile Services', and 'NI-ICS', each with a dropdown arrow. At the bottom are two buttons: 'Back' and 'Create incident'.

Figure 18: Create Storm Incident

On ticking “Storm” the following page, shown in Figure 19, will appear:

- 3) In this page, provide the relevant information. Depending on the services affected (Fixed services, Mobile services, or Both), the provided information should include:
 - 3.1) an estimate of the number of users affected for each service;
 - 3.2) the number of nodes or base stations (“BS”) affected; and
 - 3.3) in the free text box, a brief description of all of the locations affected (Counties) and causes of the outage.

The screenshot shows a web form titled "Services Affected" with a blue header bar. The form is divided into four sections: "Fixed Data", "Fixed Voice", "Mobile Data", and "Mobile Voice". Each section contains two input fields for "No. of users affected" and "No. of Nodes / Base Stations affected", both showing "0". Below each section is a large text area for "Notes including main causes of outages". Three callouts are present: 3.1 points to the "No. of users affected" field in the "Fixed Data" section; 3.2 points to the "No. of Nodes / Base Stations affected" field in the "Fixed Data" section; and 3.3 points to the "Notes including main causes of outages" text area in the "Fixed Data" section.

Services Affected

3.1

Fixed Data

No. of users affected
0

No. of Nodes / Base Stations affected
0

3.2

Notes including main causes of outages

3.3

Fixed Voice

No. of users affected
0

No. of Nodes / Base Stations affected
0

Notes including main causes of outages

Mobile Data

No. of users affected
0

No. of Nodes / Base Stations affected
0

Notes including main causes of outages

Mobile Voice

No. of users affected
0

No. of Nodes / Base Stations affected
0

Notes including main causes of outages

Figure 19: Strom Report required Information

- 4) Leave the ticked option "No" in the lower half of the page (Figure 20 below) as default. Please note, as a default the "No" option is always ticked. When reporting a storm, the user is not required to make any changes to these default options;
- 5) Click on "Create Incident" when the required information has been provided.

The form is titled "Fixed Services" at the top. It contains three sections: "ECAS", "Data Service", and "Voice Service". Each section has a "Yes" radio button and a "No" radio button, with "No" selected. A green bracket labeled "4" groups the "Mobile Services" section, which also has "ECAS", "Data Service", and "Voice Service" sections with "No" selected. A green arrow labeled "5" points from the "Create incident" button at the bottom right.

Fixed Services

ECAS

☐ Yes ☒ No

Data Service

☐ Yes ☒ No

Voice Service

☐ Yes ☒ No

Mobile Services

ECAS

☐ Yes ☒ No

Data Service

☐ Yes ☒ No

Voice Service

☐ Yes ☒ No

NI-ICS

ECAS

☐ Yes ☒ No

Data Service

☐ Yes ☒ No

Voice Service

☐ Yes ☒ No

Back

Create incident

Figure 20: Storm Report Default Options – No changes Required

After steps 1 to 5 above have been completed and the function “Create Report” has been clicked, a pop-up window called ***Incident Created*** will appear, giving the user two options, “Update Incident Report now”, or “Update Incident Report later” – this is shown in Figure 21 below.

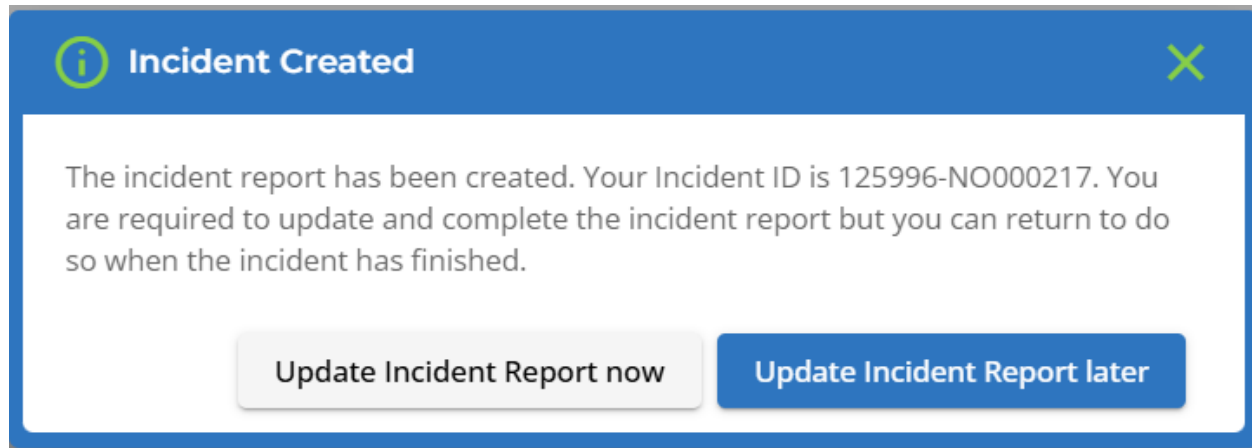


Figure 21: Incident Created Window

Section 4.2 below, provides the steps that are required to update a storm report.

4.2 Update Storm Incident Report

While a named storm or weather event and its Orange¹⁴ or Red level warning continues, operators are required to provide and continue providing updates on impact of the storm twice a day at the times of 10H00 and 16H00.

An existing storm report can be updated by logging into the **Network Incident Reporting – incident list** page. From the Incident list, the report to be updated can be chosen. Note that, any storm report will be represented visually with an Icon (as shown in Figure 22 below) to differentiate it from isolated and malicious incidents.

The required steps to update a storm report as follows:

- 1) As shown in Figure 22 below, click on “Update”;

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Action
125996-NO000217	09/09/2025, 12:00		Storm Incident Report Test	Open	Ihab Zine	Update
125996-NO000216	08/09/2025, 12:00	08/09/2025, 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000204	12/05/2025, 00:00	12/05/2025, 01:00	da	Closed	Mark Kane	
125996-NO000203	11/05/2025, 02:00	11/05/2025, 03:30	HLR Down	Closed	Mark Kane	
125996-NO000208	11/06/2025, 00:30	11/06/2025, 02:00	Iso to Mali	Closed	Ihab Zine	
125996-NO000207	11/06/2025, 00:30	11/06/2025, 01:00	Malicious test 11 June 25	Closed	Ihab Zine	
125996-NO000206	11/06/2025, 00:00	11/06/2025, 04:00	Storm Test 11 June 25	Closed	Ihab Zine	
125996-NO000205	11/06/2025, 00:00	11/06/2025, 01:00	Test 11 June 25	Closed	Ihab Zine	
125996-NO000202	07/05/2025, 06:30		Test Type Change	Open	Darren Nulty	Update
125996-NO000201	30/04/2025, 06:00	30/04/2025, 06:30	Test Incident	Closed	Darren Nulty	

Items per page: 10

1 - 10 of 22

For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.

Figure 22: Network Incident Reporting – Incident list Page

- 2) Next, the **Update Incident Report** page will appear – Figure 23 – in this page update the following information:

- 2.1) an estimate of the number of users affected for each service;

- 2.2) the number of nodes¹⁵ or base stations (“BS”) affected; and
- 2.3) In the free text box, a brief description of the locations affected (Counties) and causes of the outage.

The screenshot shows a web form titled "Services Affected" with a collapse icon in the top right. The form is organized into four distinct sections, each with a blue header:

- Fixed Data:** Contains two input fields for "No. of users affected" and "No. of Nodes / Base Stations affected", both with the value "0". Below them is a large text area for "Notes including main causes of outages".
- Fixed Voice:** Contains two input fields for "No. of users affected" and "No. of Nodes / Base Stations affected", both with the value "0". Below them is a large text area for "Notes including main causes of outages".
- Mobile Data:** Contains two input fields for "No. of users affected" and "No. of Nodes / Base Stations affected", both with the value "0". Below them is a large text area for "Notes including main causes of outages".
- Mobile Voice:** Contains two input fields for "No. of users affected" and "No. of Nodes / Base Stations affected", both with the value "0". Below them is a large text area for "Notes including main causes of outages".

Figure 23: Update Incident Report Page for Storm Reporting

- 3) To exit from the **Update Incident Report** page, click on “Save Changes”, then click on “Home Icon” function. The user will be routed back to the **Network Incident Reporting – Incident list** page.

¹⁵ In the case of the Fixed Service or NI-ICS this includes but is not limited to: Points of Presence, Data centres, Interconnect points etc.,

Section 4.3 below, provides the steps that are required to close a storm report.

4.3 Close Storm Incident Report

Once a named storm or weather event and its Orange¹⁴ (or above) level warning is no longer in operation and the operator's networks and services have returned to Business as Usual ("BAU")¹⁶, the storm report can be closed. To do so, the required steps as follows (Figure 24):

- 1) Provide the end date and time of the storm report;
- 2) Provide information on Incident Response and actions taken; and
- 3) Finally, provide information on Root Cause Analysis, Mitigations and Timescale.

The screenshot displays the 'Update Incident Report' interface. At the top, a blue header bar contains the title 'Update Incident Report'. Below this, a summary bar shows 'Summary 125996-NO000217', 'Incident Type: Storm', and 'Reporter: Ihab Zine'. The main form area includes several sections: 'Title*' with the value 'Storm Incident Report Test'; 'Start Date and Time of Incident:' with a date of '09/09/2025' and a time of '12:00'; 'End Date and Time of Incident:' with a date field and a time field; 'Duration: 0 days'; 'Sub Categories:' with checkboxes for 'Authenticity', 'Availability' (checked), 'Confidentiality', and 'Integrity'; 'Description of incident*' with the text 'This Storm Incident is created as a demo'; 'Incident Response and Actions Taken'; and 'Root Cause Analysis, Mitigation Measures and Timescale'. Three green arrows with numbered boxes (1, 2, and 3) point to the 'End Date and Time of Incident:' section, the 'Incident Response and Actions Taken' section, and the 'Root Cause Analysis, Mitigation Measures and Timescale' section, respectively, indicating the required steps for closure.

Figure 24: Update Incident Report page – Information Required for closure

¹⁶ Less than 1% of the National User Base affected and no particular geographic concentration.

- 4) Next, click on "Save Changes", then click on "Close Incident".

A pop-up window called **Incident Closed** will appear to confirm that the report has been closed successfully as shown in Figure 25 below.

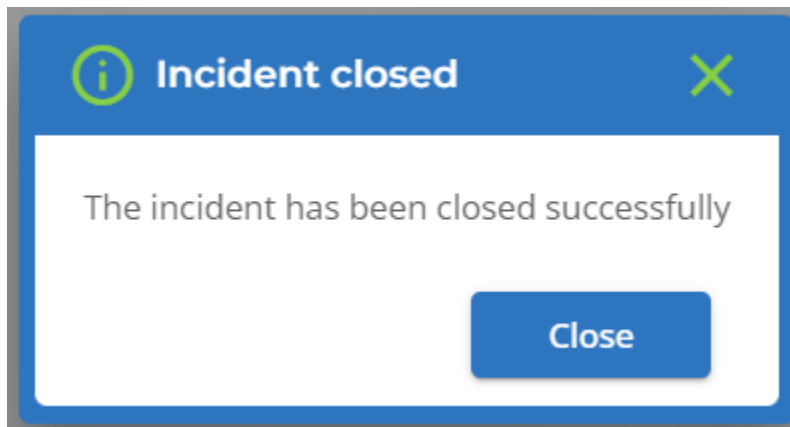


Figure 25: Incident Closed window

Once the storm report has been closed, the update function will be deactivated and the status of the incident report will be indicated as closed, as shown in Figure 26 below.

Network Incident Reporting - Incident list						
Search Incidents:		Show All	Help / Instructions		New incident	
Incident Id	Start date/time	End date/time	Title	Status	Reporter	Action
125996-NO000217	09/09/2025, 10:30	09/09/2025, 11:00	Storm Incident Report Test	Closed	Ihab Zine	
125996-NO000216	08/09/2025, 12:00	08/09/2025, 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000204	12/05/2025, 00:00	12/05/2025, 01:00	da	Closed	Mark Kane	
125996-NO000203	11/05/2025, 02:00	11/05/2025, 03:30	HLR Down	Closed	Mark Kane	
125996-NO000208	11/06/2025, 00:30	11/06/2025, 02:00	Iso to Mali	Closed	Ihab Zine	

Items per page: 5

1 - 5 of 22

For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.

Figure 26: Network Incident Reporting – Incident list Page – Closed Storm Incident