



An Coimisiún um  
**Rialáil Cumarsáide**  
Commission for  
**Communications Regulation**

# Network Incidents

## Users' Guide for ComReg's Portal for Reporting Security Incidents

### Information Notice

**Reference:** ComReg 24/41

**Version:** Final

**Date:** 31/05/2024

**An Coimisiún um Rialáil Cumarsáide**  
**Commission for Communications Regulation**

1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.  
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.  
Teil | Tel +353 1 804 9600 Suíomh | Web [www.comreg.ie](http://www.comreg.ie)

**Additional Information**

Document No:	24/41
Date:	31/05/2024

# Content

Section	Page
1: Introduction.....	4
1.1 Background.....	4
1.2 Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 .....	4
1.3 Structure of this document .....	6
2: Account Creation and Logging In .....	7
3: Reporting Security Incidents .....	12
3.1 Reporting a new Security Incident .....	12
3.2 Update a security Incident Report.....	18
3.3 Close a security Incident Report .....	22
4: Storm Incidents Reporting.....	26
4.1 Report new Storm Incident.....	26
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 resource<sup>1</sup>.

The on-line portal for the reporting of incidents (“Portal”) was introduced in 2019 to facilitate online incident reporting while the data required by it for reporting continued to be that set out in the previous Incident Reporting Form 14/02a<sup>2</sup>. The Portal not only enabled the on-line reporting of a new incident but also facilitated the updating of information in relation to an incident 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 consultation<sup>3</sup> introducing changes to the framework for the reporting of security incidents<sup>4</sup>

---

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

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

<sup>3</sup> 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>.

<sup>4</sup> 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"). Then, in 2024, ComReg published a Response to Consultation and its associated Decision Instrument<sup>5</sup>.

Following the publication of ComReg Document 24/23 and its Decision Instrument D08/24, the Portal has been updated for consistency with these documents. The Portal now has newly added functionality, including:

- 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.

This document ComReg 24/41 is the user's guide for ComReg's Portal for reporting security incidents affecting providers of ECN, ECS and NI-ICS and replaces ComReg 19/98<sup>6</sup>.

While the document structure is similar to its predecessor, there are some notable changes including:

- updated security incident type selections ('Isolated', 'Storm', or 'Malicious');
- new security incident sub-categories (Authenticity, Availability, Confidentiality, or Integrity);
- the addition of NI-ICS provider services; and
- updated asset types reflecting modern networks and services.

---

<sup>5</sup> 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>

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

### 1.3 Structure of this document

This document is structured as follow:

- Section 2 (Account Activation and First Login), provides the URL and 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 button<sup>7</sup> functions to press are indicated as below:

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

In case of issues using the Portal, and for further questions, please contact ComReg via the following dedicated email ([incident@comreg.ie](mailto:incident@comreg.ie)).

---

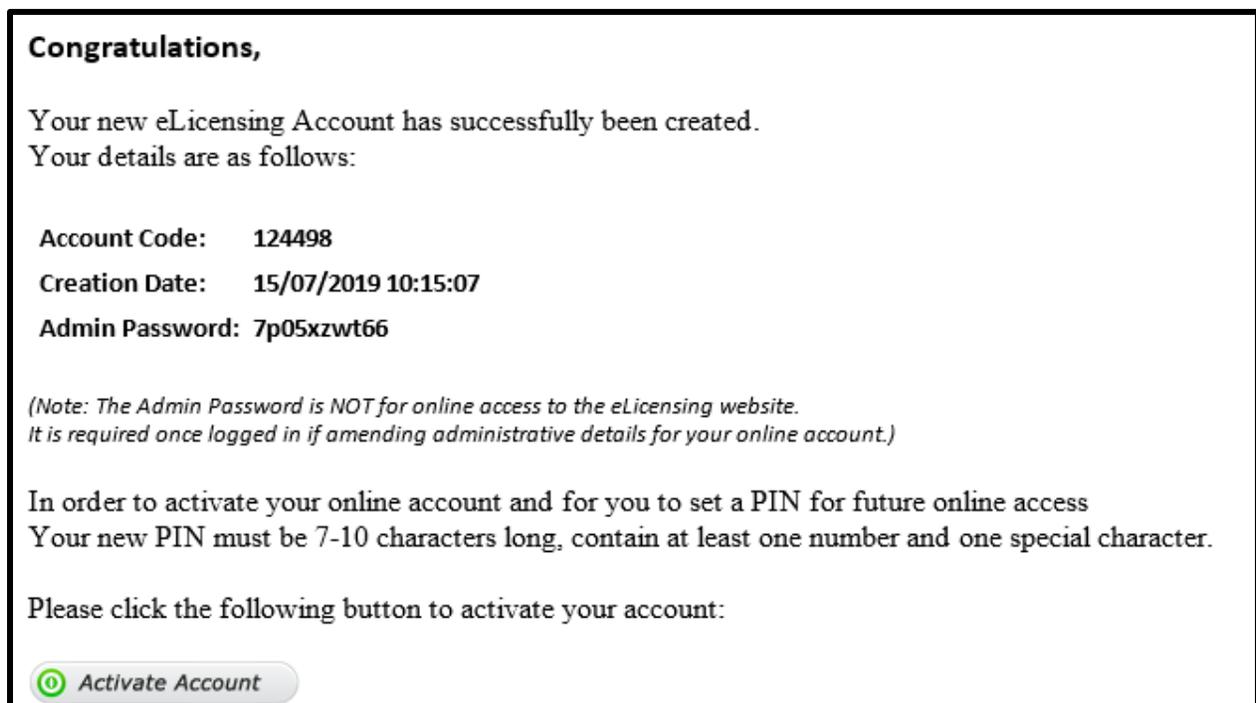
<sup>7</sup> All functionality is accessed by clicking on tagged buttons on each part of the form. The guide takes the operator through the steps, including buttons to press, to report an incident.

## 2: Account Creation and Logging In

When registering to use the Portal for the first time<sup>8</sup>, 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](mailto:incident@comreg.ie)):

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

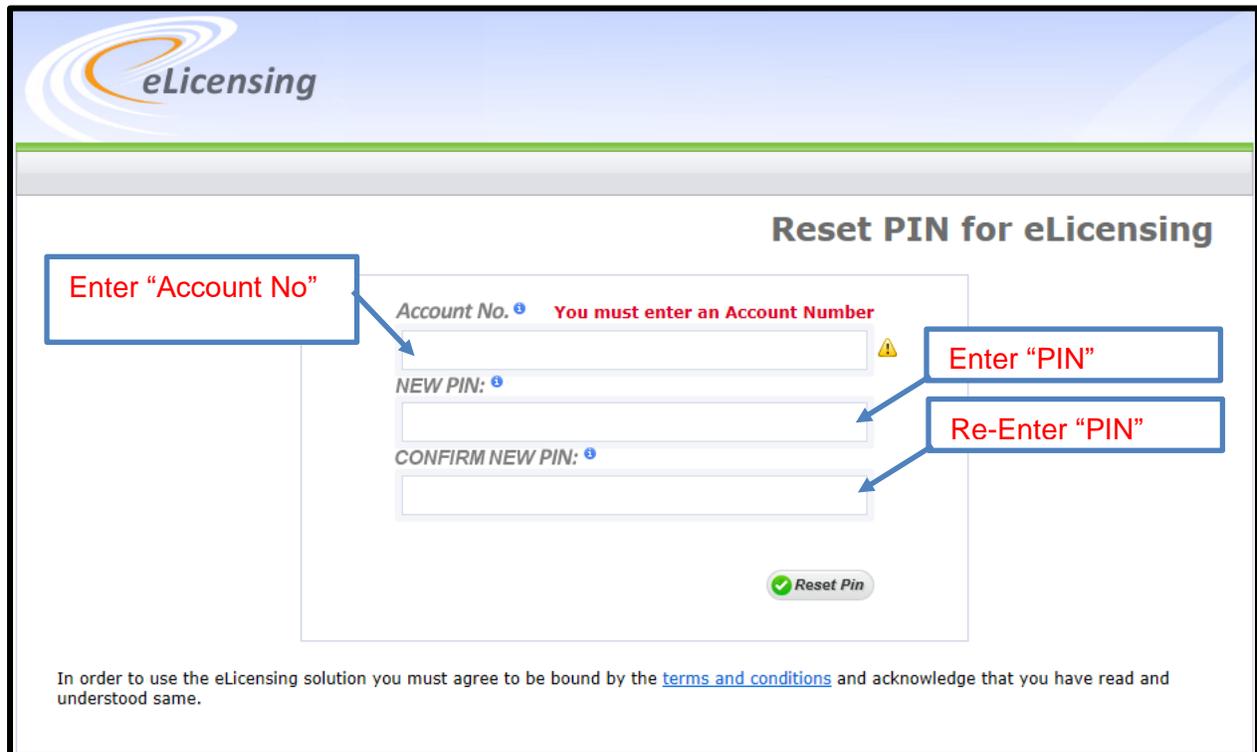
After ComReg creates the account, an email will be sent to the contact person(s) advising them of the account creation and with instructions as to how to activate the account. A screenshot of the email template is shown below:



**Figure 1: Email Confirming Account Creation**

<sup>8</sup> Existing users do not need to re-register to use the updated Portal. They can use their existing account number and PIN to login and use the Portal.

Clicking on the “Activate Account” function (Figure 1 above), will redirect the user to the **Reset PIN for eLicensing** page. The user inputs the newly generated account code and the new PIN. The new PIN must be 7-10 characters long, containing at least one number and one special character. A screenshot of the **Reset PIN for eLicensing** page is shown in Figure 2 below. **Please Note**, if a company wishes to assign multiple users to use the Portal, the users will need to share and use the same PIN (7-10 characters), therefore, it is advised to use a strong, unique PIN. Choose a PIN that is unique from any PIN you have previously used.



**Reset PIN for eLicensing**

Enter "Account No"

Account No. <sup>?</sup> You must enter an Account Number

NEW PIN: <sup>?</sup>

CONFIRM NEW PIN: <sup>?</sup>

Enter "PIN"

Re-Enter "PIN"

Reset Pin

In order to use the eLicensing solution you must agree to be bound by the [terms and conditions](#) and acknowledge that you have read and understood same.

**Figure 2: Reset PIN for eLicensing Page**

After resetting the PIN, a new page will open, advising the user that the eLicensing account has been successfully activated, as shown in Figure 3 below.

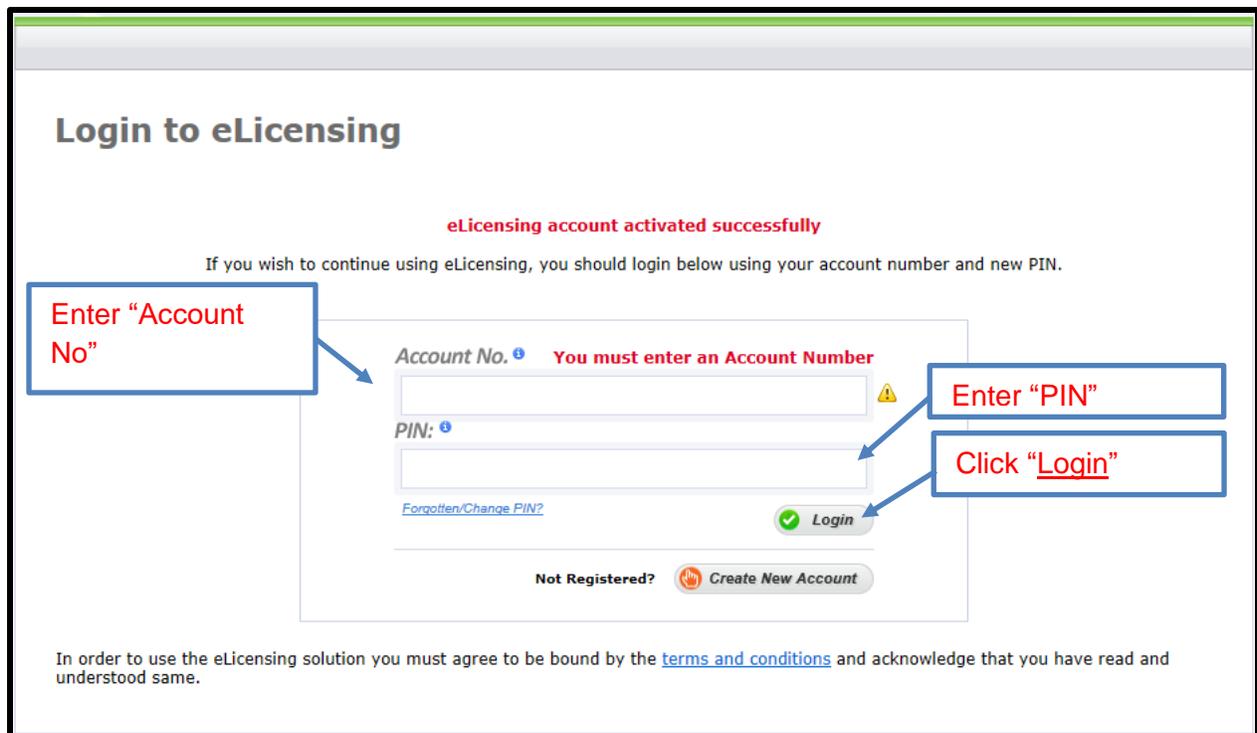


Figure 3: eLicensing Account Activation

The user can now login to the Portal. The user will be asked to provide the “Account No.” and “PIN”. After clicking the “Login” function, the user will be asked to read and accept the terms and conditions of the eLicensing website when logging in for the first time. Figure 4 below shows a screenshot of this page.

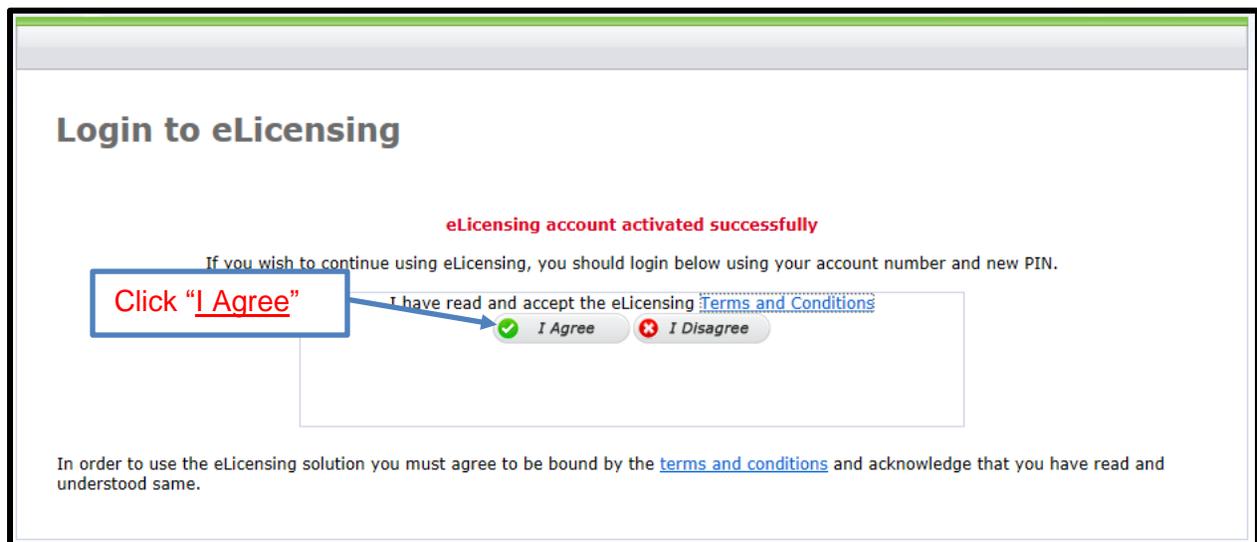


Figure 4: eLicensing Terms and Conditions Page

As part of two-factor authentication, the user will then be asked to select their name from the dropdown list and click on "Request Authentication Code" as shown in Figure 5 below.

**Login to eLicensing - Step 2**

In order to establish your user credentials, please select your name from the dropdown list below and request an authentication code. An email with an authentication code will be sent to the selected contact.

**User**

-- Select Contact --

Only Contacts with an assigned email address are displayed.  
If you wish to amend any of your Contact Details, please contact the Network Operations Unit at [NetworkOps@comreg.ie](mailto:NetworkOps@comreg.ie).

In order to use the eLicensing solution you must agree to be bound by the [Terms and Conditions](#) and acknowledge that you have read and understood the same.

**Figure 5: eLicensing Login – Two-Factor Authentication**

The authentication code, which will be valid for 10 minutes, is then sent to the registered email address associated with the user. In the **Login to eLicensing – Step 3** page, input this authentication code to the field and click on "Complete Login", as shown in Figure 6 below.

**Login to eLicensing - Step 3**

Please enter the authentication code that has been emailed to the selected contact email address below, and click the Complete Log in button to authenticate your log in. Note that the authentication code will expire after 12 hours.

**User**

Test UAT Account      marianne.macbean@comreg.ie

**Authentication Code**

.....

In order to use the eLicensing solution you must agree to be bound by the [Terms and Conditions](#) and acknowledge that you have read and understood the same.

**Figure 6: eLicensing Login – Two-Factor Authentication**

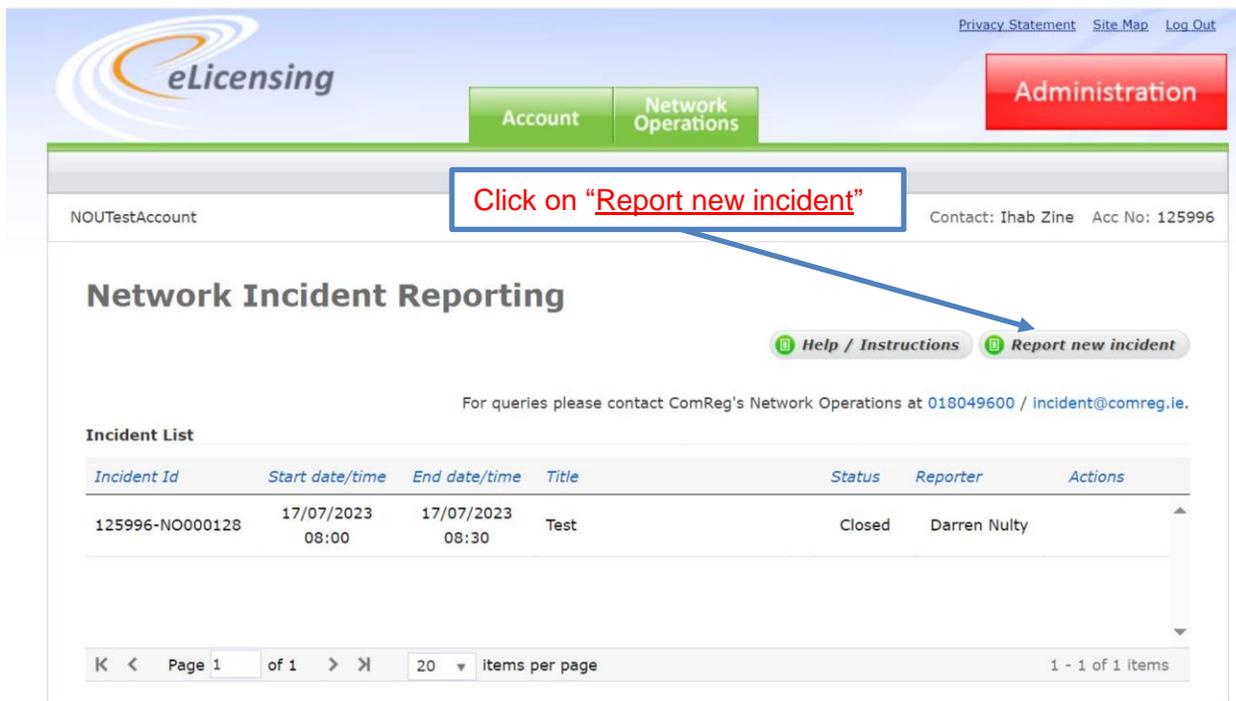
The user is now routed to the ***Network Incident Reporting*** page.

## 3: Reporting Security Incidents<sup>9</sup>

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

### 3.1 Reporting a new Security Incident

In order, to create a new security incident report, click on "Report new incident" as shown in Figure 7 below.



The screenshot displays the 'Network Incident Reporting' page. At the top, there is a navigation bar with 'Account', 'Network Operations', and 'Administration' buttons. Below this, the page title 'Network Incident Reporting' is visible, along with a 'Report new incident' button highlighted by a red box and a blue arrow. A table below shows an incident list with columns for Incident Id, Start date/time, End date/time, Title, Status, Reporter, and Actions. The table contains one row with incident ID 125996-NO000128, start time 17/07/2023 08:00, end time 17/07/2023 08:30, title 'Test', status 'Closed', and reporter 'Darren Nulty'.

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Actions
125996-NO000128	17/07/2023 08:00	17/07/2023 08:30	Test	Closed	Darren Nulty	

Figure 7: Network Incident Reporting Page

<sup>9</sup> 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, relevant to each 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 Malicious<sup>10</sup>)
- 2) Select the sub-category<sup>11</sup> (Authenticity, Availability, Confidentiality, or Integrity).
- 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 (or both), or NI-ICS Services; and
- 5) Click on "Create Report" when the required information has been provided.

---

<sup>10</sup> This type is intended to catch security incidents including but 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.).

<sup>11</sup> a security incident may feature more than a single sub-category. Therefore, providers should use any or all of the sub-categories that accurately describe the security incident in progress.

### CREATE INCIDENT REPORT

**SUMMARY** 1)

Incident Type:  Isolated  Storm  Malicious

Title:

Start Date and Time of Incident: **Time:**  **Date:**

Sub Categories: 2)  Authenticity  Availability  Confidentiality  Integrity

Description of incident:

**Fixed Services** 3)

ECAS Affected  Yes  No

Data Service Affected  Yes  No

Voice Service Affected  Yes  No

**Mobile Services** 4)

ECAS Affected  Yes  No

Data Service Affected  Yes  No

Voice Service Affected  Yes  No

**NI-ICS**

ECAS Affected  Yes  No

Data Service Affected  Yes  No

Voice Service Affected  Yes  No

5)

Figure 8: Create Incident Report Page

Note that when the user ticks the "Yes" box for Fixed Services, Mobile Services, 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 Affected, as shown in Figure 9 below.

### CREATE INCIDENT REPORT

**SUMMARY**

Incident Type:  Isolated  Storm  Malicious

Title:

Start Date and Time of Incident: **Time:**  **Date:**

Sub Categories:  Authenticity  Availability  Confidentiality  Integrity

Description of incident: 

This security incident is created for the purpose of demonstration.  
 The incident type selected is Isolated  
 The sub-categories selected are Authenticity and Availability.

**Fixed Services**

ECAS Affected  Yes  No

Data Service Affected  Yes  No

Voice Service Affected  Yes  No

**Mobile Services**

ECAS Affected  Yes  No

Data Service Affected  Yes  No

Service Offering(s) Affected  Retail

Number of End Users Affected

Quantity of Sites Affected

\_\_\_\_\_

Wholesale

Voice Service Affected  Yes  No

Service Offering(s) Affected  Retail  Wholesale

**NI-ICS**

ECAS Affected  Yes  No

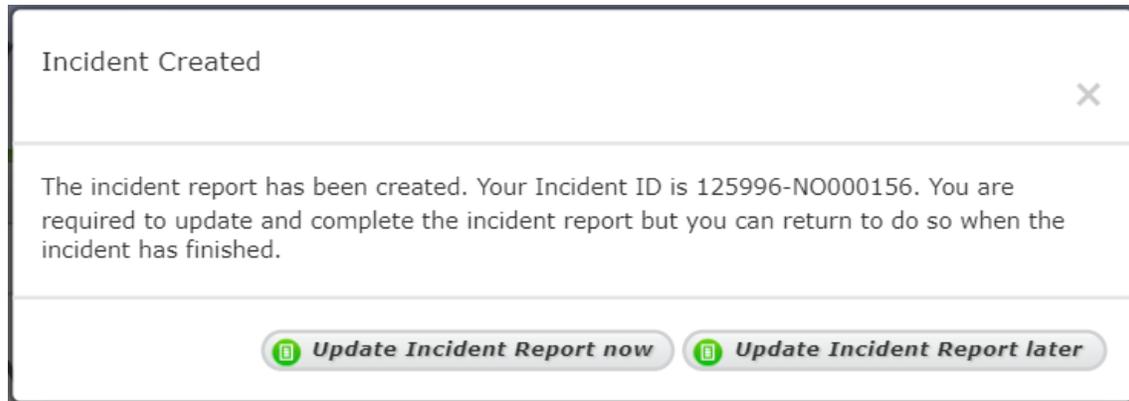
Data Service Affected  Yes  No

Voice Service Affected  Yes  No

Create Report

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

After Steps 1 to 5 on page 14 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.

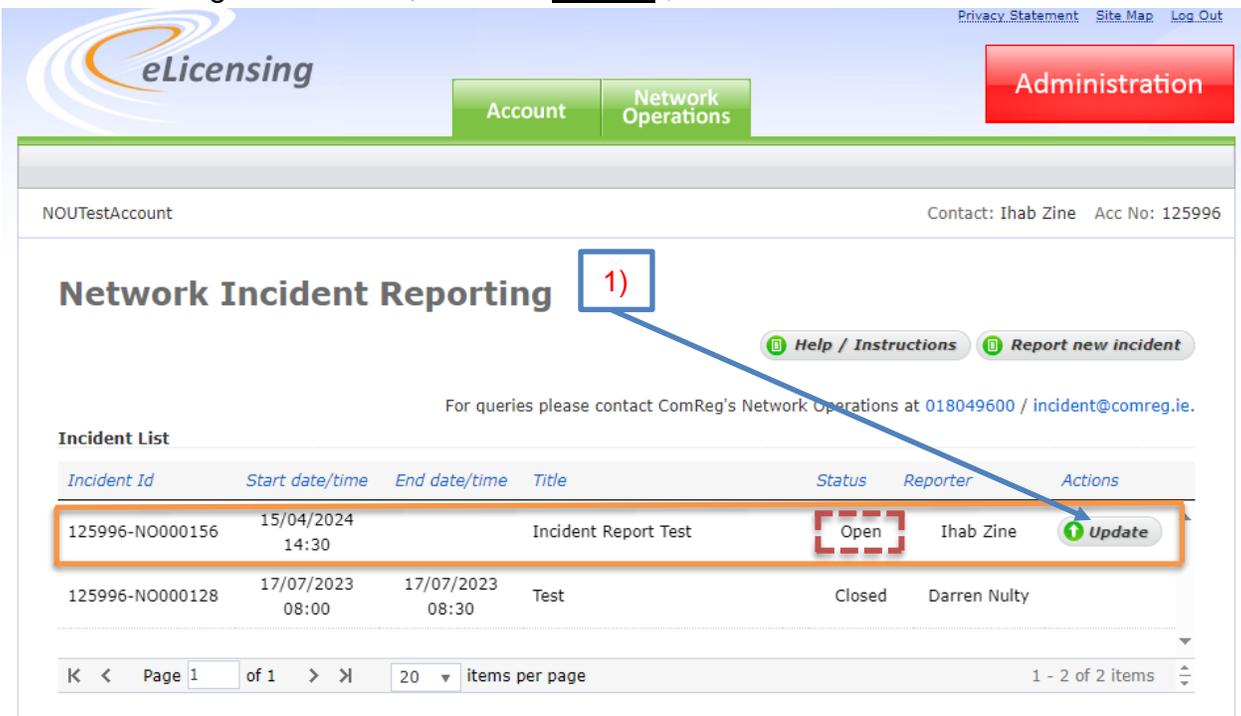
## 3.2 Update a security Incident Report

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

An existing security incident report can be updated by logging into the **Network Incident Reporting** page. From the Incident List, the report to be updated can be chosen. 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 as follows:

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



The screenshot displays the 'Network Incident Reporting' page. At the top, there is a navigation bar with the 'eLicensing' logo, 'Account', 'Network Operations', and 'Administration' buttons. Below the navigation bar, the user's account information is shown: 'NOUtestAccount' and 'Contact: Ihab Zine Acc No: 125996'. The main heading is 'Network Incident Reporting', with a red box and '1)' pointing to it. Below the heading are links for 'Help / Instructions' and 'Report new incident'. A message states: 'For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.' The 'Incident List' table is shown below, with the first row highlighted in orange. The first row contains the following data: Incident Id: 125996-NO000156, Start date/time: 15/04/2024 14:30, End date/time: (blank), Title: Incident Report Test, Status: Open, Reporter: Ihab Zine, and Actions: Update. The 'Update' button is highlighted with a red dashed box. The second row contains: Incident Id: 125996-NO000128, Start date/time: 17/07/2023 08:00, End date/time: 17/07/2023 08:30, Title: Test, Status: Closed, Reporter: Darren Nulty, and Actions: (blank). At the bottom, there is a pagination control showing 'Page 1 of 1' and '20 items per page'.

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Actions
125996-NO000156	15/04/2024 14:30		Incident Report Test	Open	Ihab Zine	Update
125996-NO000128	17/07/2023 08:00	17/07/2023 08:30	Test	Closed	Darren Nulty	

Figure 11: Network Incident Reporting Page

- 2) Next, in the **Incident Details** 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 **Incident Details** page, click on “Network Operations” function. The user will be routed back to the **Network Incident Reporting** page.

## INCIDENT DETAILS

SUMMARY 125996-NO000156

Reporter: **Ihab Zine**

[Hide detail](#)

**Title:**

**Start Date and Time of Incident:** **Time:**  **Date:**

**End Date and Time of Incident:** **Time:**  **Date:**

**Duration:** **0 days**

**Sub Categories:**  **Authenticity**  **Availability**  **Confidentiality**  **Integrity**

**Description of incident:**

This security incident is created for the purpose of demonstration.

The incident type selected is Isolated

The sub-categories selected are Authenticity and Availability.

**Incident Response and Actions Taken:**

**Root Cause Analysis, Mitigation Measures and Timescale:**

### Fixed Services

**ECAS Affected**  Yes  No

**Data Service Affected**  Yes  No

**Voice Service Affected**  Yes  No

Figure 12: Incident Details Page (a)

**Mobile Services**

**ECAS Affected**  Yes  No

**Data Service Affected**  Yes  No [Hide details](#)

**Service Offering(s) Affected**  Retail

Number of End Users Affected

Quantity of Sites Affected

---

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	

**Asset(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"/> Fibre	<input type="checkbox"/> DNS	<input type="checkbox"/> DSLAM
<input type="checkbox"/> Interconnect	<input type="checkbox"/> Firewall	<input type="checkbox"/> Gateway
<input type="checkbox"/> Router	<input type="checkbox"/> Network Control	<input type="checkbox"/> Radio
<input type="checkbox"/> Signalling Diameter	<input type="checkbox"/> Server	<input type="checkbox"/> Signalling SS7
<input type="checkbox"/> SIP	<input type="checkbox"/> Signalling Radius	<input type="checkbox"/> Signalling Other
<input type="checkbox"/> Wholesale Services	<input type="checkbox"/> Switch	<input type="checkbox"/> VoIP/VoLTENode

5G Core:

<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 Cause**

- Cooling Failure
- Malicious Actions
- Natural Phenomena
- Power Failure
- System Failure
- Third Party Failure
- Other

**Voice Service Affected**  Yes  No

**NI-ICS**

**ECAS Affected**  Yes  No

**Data Service Affected**  Yes  No

**Voice Service Affected**  Yes  No

2)

Figure 13: Incident Details Page (b)

If the security incident has ended, and the root cause analysis has been satisfactorily completed by the user concerned to ComReg's satisfaction, then the user can follow the required steps in sub-section 3.3 below to close the security incident report.

### 3.3 Close 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.

**Mobile Services**

**ECAS Affected**  Yes  No

**Data Service Affected**  Yes  No [Hide details](#)

**Service Offering(s) Affected**  Retail

Number of End Users Affected

Quantity of Sites Affected

---

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	

**Asset(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"/> Fibre	<input type="checkbox"/> DNS	<input type="checkbox"/> DSLAM
<input type="checkbox"/> Interconnect	<input type="checkbox"/> Firewall	<input type="checkbox"/> Gateway
<input type="checkbox"/> Router	<input type="checkbox"/> Network Control	<input type="checkbox"/> Radio
<input type="checkbox"/> Signalling Diameter	<input type="checkbox"/> Server	<input type="checkbox"/> Signalling SS7
<input type="checkbox"/> SIP	<input type="checkbox"/> Signalling Radius	<input type="checkbox"/> Signalling Other
<input type="checkbox"/> Wholesale Services	<input type="checkbox"/> Switch	<input type="checkbox"/> VoIP/VoLTENode

**5G Core:**

<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 Cause**

<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

**Voice Service Affected**  Yes  No

**NI-ICS**

**ECAS Affected**  Yes  No

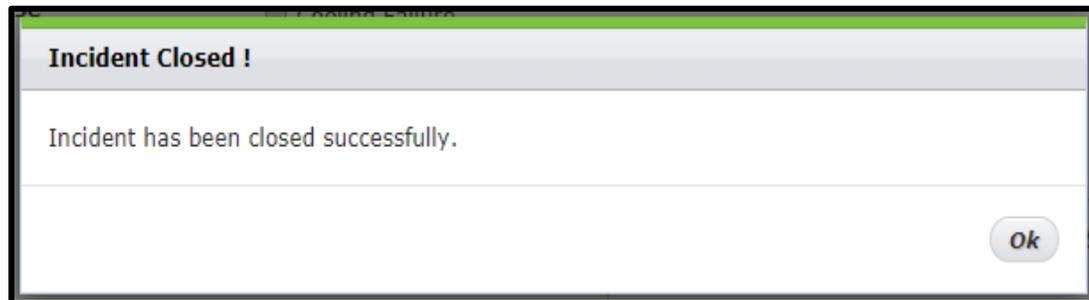
**Data Service Affected**  Yes  No

**Voice Service Affected**  Yes  No

1)
2)

Figure 14: Incident Details 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.

The screenshot displays the 'Network Incident Reporting' page. At the top, there is a navigation bar with 'Account', 'Network Operations', and 'Administration' buttons. Below this, the user's account information is shown: 'NOUTestAccount' and 'Contact: Ihab Zine Acc No: 125996'. The main heading is 'Network Incident Reporting', followed by links for 'Help / Instructions' and 'Report new incident'. A note states: 'For queries please contact ComReg's Network Operations at 018049600 / incident@comreg.ie.' Below this is an 'Incident List' table with the following data:

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Actions
125996-NO000156	15/04/2024 14:30	15/04/2024 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000128	17/07/2023 08:00	17/07/2023 08:30	Test	Closed	Darren Nulty	

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and '20 items per page'.

**Figure 16: Network Incident Reporting Page with Closed Incident**

Note that, as the security incident report has been indicated as 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: Storm Incidents Reporting

To allow for a simplified storm reporting operators are required to report storm incidents via the incident reporting portal.

When Met Éireann indicates that a named storm is expected and that Orange Level warnings<sup>12</sup> are expected 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 eLicencing Portal (as shown by Figure 5 to Figure 7 in section 2 above), the user will be routed to the **Network Incident Reporting** page, which provides the option to report a new incident.

---

<sup>12</sup> 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 "Report new incident" as shown in Figure 17below.

Privacy Statement Site Map Log Out

eLicensing

Account Network Operations Administration

NOUtestAccount Contact: Ihab Zine Acc No: 125996

Click on "Report new incident"

## Network Incident Reporting

[Help / Instructions](#) [Report new incident](#)

For queries please contact ComReg's Network Operations at 018049600 / [incident@comreg.ie](mailto:incident@comreg.ie).

### Incident List

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Actions
125996-NO000156	15/04/2024 14:30	15/04/2024 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000128	17/07/2023 08:00	17/07/2023 08:30	Test	Closed	Darren Nulty	

K < Page 1 of 1 > > 20 items per page 1 - 2 of 2 items

**Figure 17: Create Storm Report from Network Incident Reporting 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;

## CREATE INCIDENT REPORT

**SUMMARY**

Incident Type:  Isolated  Storm  Malicious

Title:

Start Date and Time of Incident: Time:  Date:

Sub Categories:  Authenticity  Availability  Confidentiality  Integrity

Description of 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 the locations affected (Counties) and causes of the outage.

**Services Affected**

<b>Fixed Data</b>	No. of users affected: <input type="text" value="0"/>	Notes including main causes of outages: <input type="text"/>
	No. of Nodes / Base Stations affected: <input type="text" value="0"/>	
<b>Fixed Voice</b>	No. of users affected: <input type="text" value="0"/>	Notes including main causes of outages: <input type="text"/>
	No. of Nodes / Base Stations affected: <input type="text" value="0"/>	
<b>Mobile Data</b>	No. of users affected: <input type="text" value="0"/>	Notes including main causes of outages: <input type="text"/>
	No. of Nodes / Base Stations affected: <input type="text" value="0"/>	
<b>Mobile Voice</b>	No. of users affected: <input type="text" value="0"/>	Notes including main causes of outages: <input type="text"/>
	No. of Nodes / Base Stations affected: <input type="text" value="0"/>	

**Figure 19: Storm 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 Report” when the required information has been provided.

**Fixed Services**

ECAS Affected  Yes  No

Data Service Affected  Yes  No

Voice Service Affected  Yes  No

**Mobile Services**

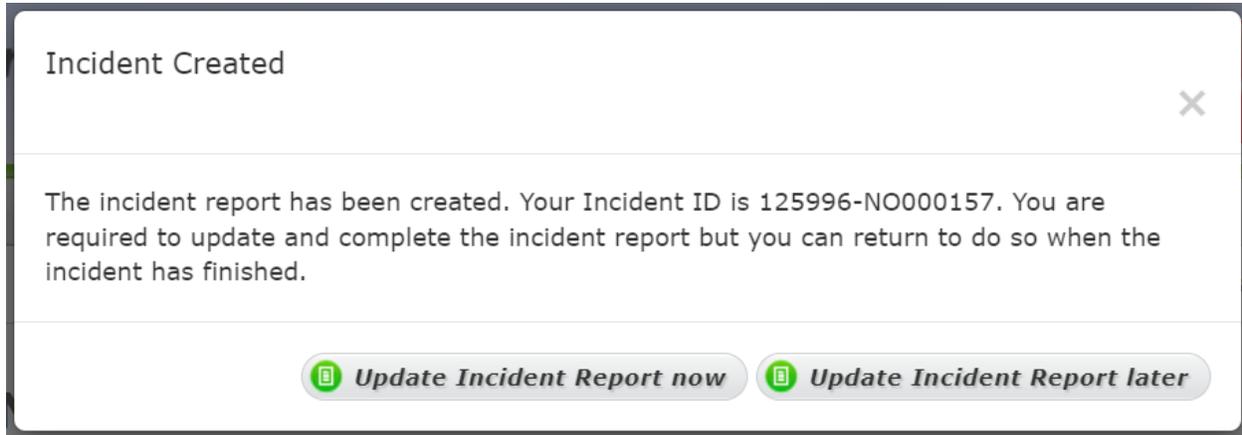
ECAS Affected  Yes  No

Data Service Affected  Yes  No

Voice Service Affected  Yes  No

**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.

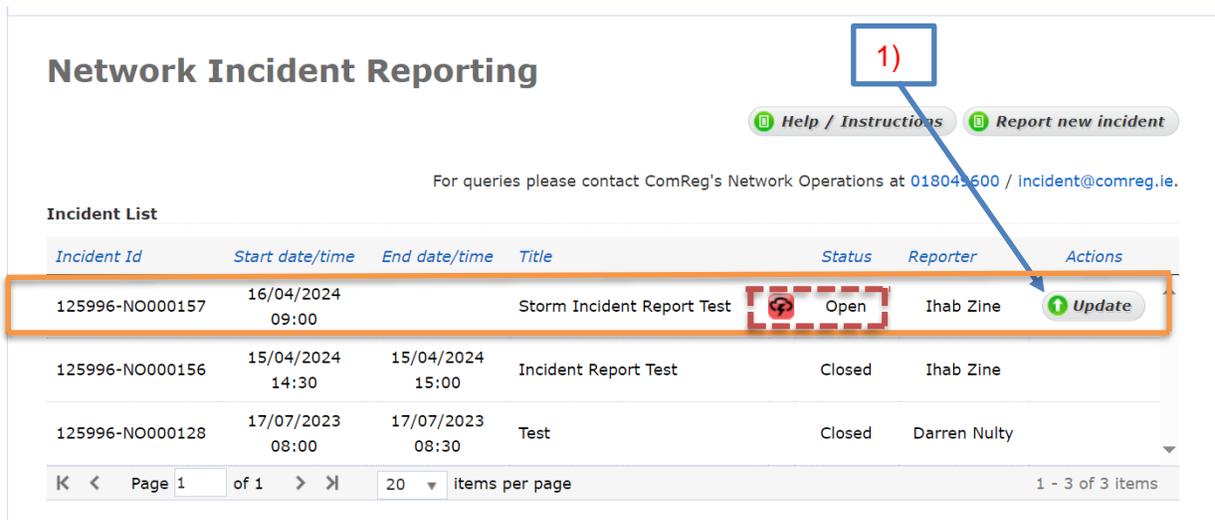
## 4.2 Update Storm Incident Report

As a named storm and its Orange<sup>12</sup> (or above) level warning remains to be in operation, 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** page. From the Incident list, the report to be updated can be chosen. Note that, any storm report will be represented visually with a badge (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”;



The screenshot shows the 'Network Incident Reporting' page. At the top, there are links for 'Help / Instructions' and 'Report new incident'. Below this, a message states: 'For queries please contact ComReg's Network Operations at 01804 5600 / incident@comreg.ie.' The main section is titled 'Incident List' and contains a table with the following data:

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Actions
125996-NO000157	16/04/2024 09:00		Storm Incident Report Test	Open	Ihab Zine	Update
125996-NO000156	15/04/2024 14:30	15/04/2024 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000128	17/07/2023 08:00	17/07/2023 08:30	Test	Closed	Darren Nulty	

At the bottom of the page, there is a pagination control showing 'Page 1 of 1' and '20 items per page'. The 'Update' button for the first incident is highlighted with a red dashed box, and a blue box with the number '1)' has an arrow pointing to it.

Figure 22: Network Incident Reporting Page

- 2) Next, the **Incident Details** 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 nodes 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.

**Services Affected**

<b>Fixed Data</b>	No. of users affected: <input style="width: 100px;" type="text" value="0"/> No. of Nodes / Base Stations affected: <input style="width: 100px;" type="text" value="0"/>	Notes including main causes of outages:	<input style="width: 100%; height: 40px;" type="text"/>
<b>Fixed Voice</b>	No. of users affected: <input style="width: 100px;" type="text" value="0"/> No. of Nodes / Base Stations affected: <input style="width: 100px;" type="text" value="0"/>	Notes including main causes of outages:	<input style="width: 100%; height: 40px;" type="text"/>
<b>Mobile Data</b>	No. of users affected: <input style="width: 100px;" type="text" value="0"/> No. of Nodes / Base Stations affected: <input style="width: 100px;" type="text" value="0"/>	Notes including main causes of outages:	<input style="width: 100%; height: 40px;" type="text"/>
<b>Mobile Voice</b>	No. of users affected: <input style="width: 100px;" type="text" value="0"/> No. of Nodes / Base Stations affected: <input style="width: 100px;" type="text" value="0"/>	Notes including main causes of outages:	<input style="width: 100%; height: 40px;" type="text"/>

**Figure 23: Incident Details Page for Storm Reporting**

- 3) To exit from the **Incident Details** page, click on “Save Changes”, then click on “Network Operations” function. The user will be routed back to the **Network Incident Reporting** page.

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

## 4.3 Close Storm Incident Report

As a named storm and its Orange<sup>12</sup> (or above) level warning is no longer in operation and the operator's networks and services have returned to Business as Usual, 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.

## INCIDENT DETAILS

**SUMMARY** 125996-NO000157  Storm Incident Reporter: Ihab Zine [Hide detail](#)

Title:

Start Date and Time of Incident: Time:  Date:

End Date and Time of Incident: Time:  Date:

Duration  **1)**

Sub Categories:  Authenticity  Availability  Confidentiality  Integrity

Description of Incident:

Incident Response and Actions Taken:

Root Cause Analysis, Mitigation Measures and Timescale:

**2)**

**3)**

**Figure 24: Incident Details – Information Required for closure**

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.

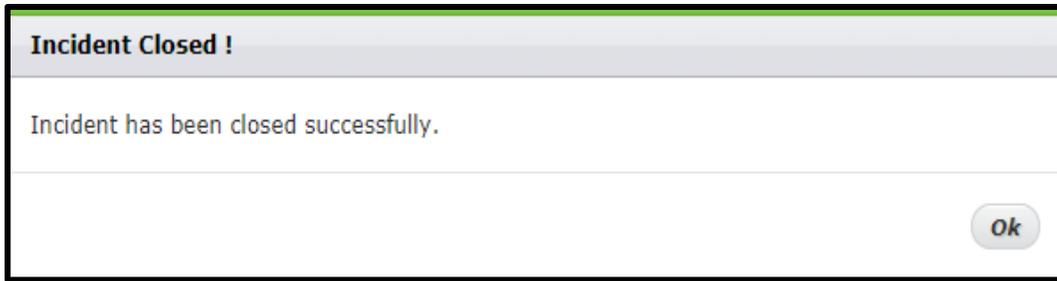


Figure 25: Incident Closed window

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**

[Help / Instructions](#)   [Report new incident](#)

For queries please contact ComReg's Network Operations at [018049600](tel:018049600) / [incident@comreg.ie](mailto:incident@comreg.ie).

**Incident List**

Incident Id	Start date/time	End date/time	Title	Status	Reporter	Actions
125996-NO000157	16/04/2024 09:00	16/04/2024 12:00	Storm Incident Report Test	 Closed	Ihab Zine	
125996-NO000156	15/04/2024 14:30	15/04/2024 15:00	Incident Report Test	Closed	Ihab Zine	
125996-NO000128	17/07/2023 08:00	17/07/2023 08:30	Test	Closed	Darren Nulty	

K < Page 1 of 1 > X 20 Items per page 1 - 3 of 3 items

Figure 26: Network Incident Reporting Page – Closed Storm Incident