Incident Notification Form

1. Provider name	*The full name of the provider.*
2. Provider security compromise reference number	*A unique reference number that can be used to identify the security compromise in communications with the provider.*
3. Date and time of occurrence	*When did the security compromise occur, or when first discovered.* *Expected format: DD/MM/YYYY HH:MM (24-hour format)*
4. Date and time of resolution	*When was the security compromise resolved.* *Expected format: DD/MM/YYYY HH:MM (24-hour format)* *Where the security compromise is ongoing at the time of reporting, the resolution time may be provided when it is available in a future update.*
5. Current incident status	*Whether the security compromise is ongoing or resolved.*

6. Security compromise overview	*Details of the security compromise being reported.*
	Where known, details should include:
	• *How was the security compromise first detected/discovered? e.g. drop in data traffic, increase in customer complaints, alerts from monitoring/NOC etc.*
	• *High-level timeline of events up to the point of report.*
	• *If the security compromise was cyber-related, was this under SECTION 105K (1) (a) and/or SECTION 105K (1) (b)*
	• *Root cause (if known)*
	  ○ *For cyber-type security compromises (e.g. supply chain compromise, exploitation of vulnerability, physical attack, managed service-based attack, insider attack, ransomware attack, internet routing protocol abuse, security misconfiguration, social engineering etc*
	  ○ *For resilience-type security compromises e.g. human error, severe weather, change related, power failure, cable faults, hardware faults, software faults, signalling storms, misconfiguration etc)*
	• *Actions taken to manage, contain, isolate, or resolve the security compromise.*
	• *If applicable, details of third-party causation. This should include the name of the third party and whether a service level or operational level agreement is in place with the third party and whether the security compromise affected them also.*
	• *Glossary of all terminology/nomenclature used in the submitted report.*

7. Affected services and assets	*Full details of the services affected. This should identify services as understood by the subscriber, this could include, without being limited to:* • *Broadband – FTTP, FTTC* • *VOIP/Digital Voice* • *PSTN* • *Mobile – if known impacted technologies e.g. 2G-5G* • *Satellite* *The provider should provide an overview of the networks and assets that were affected during the security compromise. At this stage the overview should be brief. Affected assets could include, without being limited to:* • *Core, Access, Backhaul* *If we decide to investigate the security compromise further, network and asset information may be required to a level of detail commensurate with the following:* • *ENISA Technical Guideline on Threats and Assets (Section 5) for legacy networks & services, and virtual/5G networks & services.* *Where possible, please inform us if any assets impacted were Network Oversight Functions (NOF), and/or Security Critical Functions (SCF)*

<table>
<tr><td>8. If applicable, effect on access to emergency services
This includes the ability to share location information.
The ability for mobile phones to roam onto available networks to make an emergency call (i.e. not dependent on their home network) should not negate the need to account for the potential impact.</td><td>Yes/No</td></tr>
<tr><td>9. Number/percentage of affected voice users (fixed line & mobile)</td><td>If a reporting threshold was met under one of the ‘percentage of users affected’ criteria, the provider should provide the number affected and the percentage of the provider’s end customers for this service that this represents.

The provider should provide details of the total number of affected customers for every service associated with a security compromise including voice and data.

Where the impact of a security compromise varies over time, effort should be made to explain how this was the case.

Where exact numbers are not available (for example, due to a mobile cell site failure), we expect the provider to use historical data to make a reasonable estimate of the number of end customers affected. Providers should take into consideration any substantial, well publicised changes in user density due to festivals, sporting events or similar.

Providers which offer wholesale products to other providers may have little or no visibility of the number of end customers affected by a security compromise with their network or service. We do not expect a provider to alter their monitoring or reporting systems to obtain this information. However, where it is clear to the provider that a security compromise is likely to result in service loss to end customers which will exceed the reporting thresholds, we would expect them to report this.

A provider should report qualifying security compromises affecting any service it sells, even if another provider fulfils the service. However, where a provider’s customers use additional services over the top of the network or service it provides, but without its direct involvement, we would not expect the provider to monitor or report any security compromises affecting such additional services.</td></tr>
<tr><td>10. Number/percentage of affected data users (fixed line & mobile)</td><td>See guidance above.</td></tr>
<tr><td>11. Location</td><td>Location information should describe the geographical location of the impact of the security compromise. Where possible, a UK postcode should be provided which identifies the geographical area where service interruption was experienced.

Where the geographical impact of a security compromise is not easily attributable to a single or small number of complete postcodes, the provider should provide a single or series of summary postcodes which will contain only the ‘outward’ part of the postcode.

Where an issue has regional or national impact, the provider should provide the name of the region or nation in lieu of a postcode.

In the case of mobile security compromises resulting in the loss of technology (e.g. 2G, 3G, 4G or 5G) or service (e.g. voice, data) at specific cell sites, a full list of the affected sites should be provided, with global cell IDs.

Use the following examples as a guide:

<table>
<tr><td>Failure location examples</td><td>Location expectation</td></tr>
<tr><td>Service interruption due to RAN failure at a single or number of cell sites</td><td>The global cell ID(s)</td></tr>
</table>
</td></tr>
</table>

	Service interruption due to failure at a single or small number of street cabinets	*The full post code of the street cabinet(s)*
	Service interruption due to issues associated with a single or a small number of exchanges	*The full post code of the exchange(s)*
	Service interruption to the whole of Leeds city centre	*The 'outward' part of the Leeds city centre post code. In this example 'LS1' would be appropriate.*
	Service interruption with impact across the whole of Manchester	*In this case the provider should report the location as 'Manchester'.*
	Service interruption with impact across an entire county/region	*In this case the provider should report the name of the county/region.*
	Service interruption with national impact	*'UK', 'England', 'Scotland', 'Wales', 'Northern Ireland', with 'north', 'south, 'east' and 'west' designations as appropriate. E.g. Northwest England.*