

# **Fibrus response to Ofcom consultation “Resilience guidance”**

## **Fibrus**

Fibrus is a local company on a mission to bring full-fibre broadband to digitally deprived and previously underserved areas of Northern Ireland and Great Britain. Founded during the global pandemic in 2019, in just three years the business has already connected over 300,000 homes by building its own network in hard-to-reach locations. Fibrus is making a significant impact on the broadband market in Northern Ireland and, more recently, is gaining strong traction in Cumbria.

The company has increased its customer base to 73,000 customers (as of January 2024), with our primary presence currently in the residential market. In 2024, Fibrus will become one of the few altnets on the market that is cashflow positive, on the strength of strong brand recognition, execution excellence and commercial focus led by an experienced senior leadership team.

## Response

Fibrus welcomes the opportunity to respond to Ofcom's consultation *Resilience guidance*. We support Ofcom's efforts to provide clarity on our obligations under Section 105 of the Communications Act.

While we broadly welcome the proposals set out in Ofcom's consultations, there are three areas we have concerns on. We set these out below in our responses to consultation questions 1 and 4.

Question 1: Do you consider the measures in the proposed guidance relating to the resilience of the physical infrastructure domains to be appropriate and proportionate?

### Definition of "security compromise"

While we agree with the broad thrust of the proposed guidance from Ofcom, we do have a concern over the interpretation of the meaning of "security compromise" as set out in paragraphs 3.5 to 3.7. Ofcom's intention is that "resilience incidents" will come within the scope of security compromises. It then sets out a broad definition of what it deems to be a resilience incident – including, *but not limited to*, outages caused by floods, cable cuts or power cuts.

This definition appears to be unnecessarily wide and may lead to unintended consequences. In particular, we are concerned that reporting obligations on smaller communication providers (CPs) could increase as all outages potentially come within the remit of a security compromise.

We currently provide an annual summary of outages as part of our Connected Nations F04 Section 135. For more serious security breaches, we would provide a separate update to Ofcom once we have established the facts. More recently, we engaged directly with Ofcom on an informal basis when we have a significant outage on our network as a result of Storms Isha and Jocelyn.

Our view is that the above represents a proportionate approach and does not impose an unreasonable administrative burden on us as a Tier 3 provider. We would welcome Ofcom confirming that it does not intend to increase reporting requirements on CPs as a result of the guidance on how it is interpreting what constitutes a security breach.

### Link aggregation group

Section 4 proposes that a CP should, wherever possible, remove single points of failure. Fibrus already designs to fulfil this requirement by, for example, providing multiple links to each optical light terminal (OLT). This utilises different routes and resilient active-active cards on the OLT.

We are planning to provide a service over Openreach's network, using its GEA product set. This involves purchasing cable links between our aggregation layer and Openreach's OLTs. The cables links sold by Openreach, however, will not allow our network to provide resilience across these links. In the event that a link fails, service would not be restored until the link is replaced by Openreach.

We have asked for Openreach to provide link aggregation group (LAG) connectivity for these cable links to ensure that the single point of failure would be removed. However, we are unaware if or when this will be provided.

Question 4: Do you consider the measures in the proposed guidance relating to communications providers' own managed services to be appropriate and proportionate?

As set out in paragraphs 4.106 to 4.110 there is a requirement to protect users of voice services by ensuring that any service disruption is kept to a minimum. Clearly, this is crucial to enable end users (particularly those who are vulnerable) to make calls to the emergency services. Accordingly, we support the policy objectives set out in this section of the consultation.

However, Ofcom will be aware of an unresolved issue regarding the porting of telephone numbers from the Openreach network to alternative VoIP providers. Because this comes with a lead time of (typically) 4 days for a single geographic number, uninterrupted service relies entirely on simultaneous porting of the number with the activation of the VoIP service. For practical purposes, this cannot always be guaranteed. For example, there may be technical or customer-led issues with the switch-on of the new service.

This increases the risk that there will be a period where a customer does not have access to a phone service. We have assessed options for this where a misalignment between number porting and service activation occurs. One could involve providing a temporary number from our own allocation while we are waiting for the customer number to be ported. This, we believe, is a sub-optimal customer experience.

We would welcome further clarity on Ofcom as to how it could support industry in meeting its obligations to voice users in this context.