# Colt Response

Colt values the opportunity to comment on Ofcom's Review of Security Guidance. We have not commented on those areas relating to mobile services as they are not applicable to Colt, but are pleased to offer the following observations:

1. Cyber security. We support a risk-based approach to the alignment of good/best practice with the '10 Steps to Cyber Security' and will continue to apply such measures where practical and where they support Colt's global business objectives.

2. Cyber Essential Plus. Colt is a global business exclusively focused on providing services to other enterprise customers. We take cyber security very seriously and continue to apply controls such as those contained within Cyber Essential Plus, where they support our strategic business aims. However, we must be wary of anchoring our approach to national standards, which may vary by jurisdiction.

3. ND1643. Colt is committed to ND1643 and will continue to work towards the current and future versions. In doing so Colt will continue to take the necessary technical and organisational measures to minimise the impact of security incidents on our interconnections.

4. Cyber vulnerability testing. Colt welcomes a strategic approach to cyber vulnerability testing and is keen to participate in such a scheme for the telecoms sector.

5. Single points of failure. Colt is acutely aware of the potential impacts of single points of failure and works hard to minimise such risks.

6. Flood & power resilience. Colt's customers rely on the availability of our networks and services. As such, resilience to power and flood impacts are strategic considerations. Flood and power outage risk are understood and mitigated against accordingly. Colt works closely with EC-RRG for a coordinated industry response to incidents regarding flooding and power, as well as participating in annual exercises. Previous scenarios include wide area flooding and power outages.

7. Outsourcing. Colt is aware of the challenges and risks that can be created through outsourcing. We seek to ensure that where activities are outsourced, all activities that have regulatory implications are reflected in the contract with the supplier. We take a risk based approach to identifying and managing and assuring the associated risks and welcome a strategic approach to the management of outsourcing risks across the sector.

8. Cyber incident reporting. Colt firmly believes that reporting of incidents will facilitate a more accurate picture of the threat landscape and thus lead to more informed decision making. However, reporting requirements must be supported by providing appropriate processes for anonymous reporting where practicable and proactive work to remove any suggestion of a 'blame culture'. Such processes are widely used in the aviation sector and health & safety and have been seen to be effective. We welcome a unified approach to cyber incident reporting.

9. Auditing. Colt acknowledges that auditing is a fundamental part of cyber security governance and assurance. However, such activities are resource intensive and can have an adverse impact on the operation of an organisation. Colt is already subject to customer audit as well as those conducted by our various external auditors. Therefore it is our view that any Ofcom audit must be conducted in line with current customer audit provisions. As such Ofcom should be required to provide a minimum of 14 days' notice of its intent to audit and should not do so more than once in a calendar

year, except where an incident may require additional audits. Furthermore, we consider that the requirement of the audited party to bear the full cost is disproportionate, especially where there is no evidence or suggestion of control failure.