Cyber Resilience

The cyber resilience of suppliers is increasingly important to the Scottish public sector. The number of cyber attacks targeting suppliers to the public sector has grown in recent years. Attacks can (intentionally or otherwise) disrupt and damage both suppliers' services and public services. Against this background, the Scottish public sector wants to ensure its suppliers have appropriate cyber security in place. That's because:

- We have a duty to prevent our public services from being disrupted by cyber attacks on suppliers; and
- We want to support our suppliers to improve their cyber security, because it's good for the sustainability and resilience of our digital economy and society.

To help improve supply chain cyber security, the Scottish public sector is being encouraged to adopt a more consistent approach. This will involve them:

- implementing a Guidance Note, which has been produced for all public sector organisations, setting out best practice from the National Cyber Security Centre (the UK technical authority on cyber security).
- encouraging all suppliers bidding for public sector contracts to ensure that they have appropriate and proportionate cyber securoty and resilience mechanisms in place
- encouraging all suppliers, where appropriate, to take advantage of the free National Cyber Security Early Warning service to help inform them of potential cyber attacks on their networks

You can find links to additional advice and support on cyber resilience in the "Support Available" section of the Supplier Journey.

If you have any questions, please contact: **cyberresilience@gov.scot**