Cyber Security

If the contract will involve, support or rely on the digital processing of information, organisations should ensure that appropriate consideration is given to potential cyber risks and their management.

Legislative requirements, including the General **Data Protection Regulation (GDPR)**, require all public sector organisations to ensure appropriate technical protections are in place when suppliers process personal data on their behalf. The Security of Network and Information Systems (NIS) Directive requires Operators of Essential Services in the devolved health and water sectors to have appropriate supply chain cyber security requirements in place.

It is recommended that public sector organisations have regard to the **Guidance Note on Supplier Cyber Security**, which embeds best practice advice from the National Cyber Security Centre and promotes a more consistent approach to the cyber security requirements placed on suppliers to the Scottish public sector.

Quickfire Guide

Quickfire Guide

Scottish Government Cyber Security Recommendations

The Cyber Security Procurement Support Tool is no longer in use, and instead the Scottish Government recommends that buyers:

1. undertake information/cyber assurance assessments
2. identify appropriate, proportionate cyber security requirements
3. seek assurances from bidders as to the extent to which they comply with these requirements, in a way that is aligned with the Guidance Note.

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