Scottish Government
Riaghaltas na h-Alba

Scottish Procurement Policy Note: SPPN 2/2020

NEW SCOTTISH PUBLIC SECTOR SUPPLIER CYBER SECURITY GUIDANCE NOTE.

Purpose

The purpose of this SPPN is to make public bodies aware of the publication of Scottish public sector supplier cyber security guidance which was published January 2020 and updated December 2023.

Key points

Framework agreements and contracts have the potential to be susceptible to cyber risks. This guidance is encouraged for use by public bodies to help them to assess their procurements for cyber risks at all stages of the procurement process.

The guidance encourages public bodies to follow the key steps and principles in it wherever possible to help ensure a consistent approach to cyber security across the Scottish public sector.

The guidance is available on the Scottish Government website.

A Digital Technology and Cyber Services Dynamic Purchasing System has been put in place and may help with implementation of this guidance. It is a one stop shop for purchasing bodies looking to buy cyber security services and resources and which can be obtained under Lot 4 Cyber Security Services.

Background

The Scottish Government published the Strategic Framework for a Cyber Resilient Scotland on 22 February 2021. This includes a commitment to enhance the cyber resilience of public sector supply chains. This guidance meets that commitment and is intended to help public bodies determine the levels of cyber risk associated with any given contract.

Contracts and framework agreements that the guidance can apply to

The guidance applies mainly to new contracts and framework agreements. For existing procurements a decision can be taken to complete an assessment retrospectively to help determine if there is a cyber security and/or data security and the processing of personal data risk. The guidance includes detailed advice about the steps that can be taken to conduct such a review.

Conclusion

The guidance encourages a proportionate and flexible approach to setting minimum security requirements for suppliers. Public bodies should continue to make their own decisions and take their own legal advice about what levels of cyber security are appropriate and practical for suppliers to deliver on a case by case basis. This includes making use of cyber security certifications and accreditations or equivalent only where appropriate and proportionate to the level of cyber risk assessed to be present in specific contracts.

Dissemination

Please bring this SPPN to the attention of all relevant staff, including those in agencies, non-departmental public bodies and other sponsored public bodies within your area of responsibility.

Contact information

The Scottish public sector supplier cyber security guidance note was produced by the Scottish Government Cyber Resilience Unit. If you have any questions please contact cyberresilience@gov.scot.

Scottish Procurement
The Scottish Government
5 Atlantic Quay
150 Broomielaw
Glasgow
G2 8LU.