ARGYLL AND BUTE COUNCIL **POLICY & RESOURCES COMMITTEE**

CUSTOMER & SUPPORT SERVICES **20 AUGUST 2015**

CONSULTATION ON PROPOSAL FOR A CYBER RESILIENCE STRATEGY FOR SCOTLAND

1.0 EXECUTIVE SUMMARY

1.1 The Scottish Government issued a consultation on a proposal for a cyber resilience strategy for Scotland in June and the deadline for responses is 28 August. The strategy sets out a compelling vision to ensure that Scotland has the ability to resist and rapidly recover from cyber incidents to benefit from the economic and personal opportunities and advantages that online technologies provide. The focus is to position cyberspace as an enabler for individuals, industry, and the public sector. The strategy supports many other strategies and programmes such as Scotland's Economic Strategy, Digital Future Strategy, Digital Justice Strategy, Curriculum for Excellence, E-Health Strategy, Equally Safe and the forthcoming Serious & Organised Crime Strategy and the Resilience Strategy. Once the strategy has been developed, a detailed action plan will follow.

1.2 The Council should welcome the development of this strategy which will help to support the implementation of our own Digital First policy.

1.3 The draft response is attached for approval.

ARGYLL AND BUTE COUNCIL **POLICY & RESOURCES COMMITTEE**

CUSTOMER & SUPPORT SERVICES **20 AUGUST 2015**

CONSULTATION ON PROPOSAL FOR A CYBER RESILIENCE STRATEGY FOR SCOTLAND

2.0 INTRODUCTION

2.1 The Scottish Government issued a consultation on a proposal for a cyber resilience strategy for Scotland in June and the deadline for responses is 28 August. The strategy sets out a compelling vision to ensure that Scotland has the ability to resist and rapidly recover from cyber incidents to benefit from the economic and personal opportunities and advantages that online technologies provide. The focus is to position cyberspace as an enabler for individuals, industry, and the public sector. The strategy supports many other strategies and programmes such as Scotland's Economic Strategy, Digital Future Strategy, Digital Justice Strategy, Curriculum for Excellence, E-Health Strategy, Equally Safe and the forthcoming Serious & Organised Crime Strategy and the Resilience Strategy. Once the strategy has been developed, a detailed action plan will follow.

3.0 RECOMMENDATIONS

3.1 Policy and Resources Committee is asked to approve the draft response attached at Appendix 1.

4.0 DETAIL

4.1 The strategy sets outs a vision "for a cyber resilient Scotland that is safe, secure and prosperous." There are 3 strategic outcomes identified:

- Our citizens are informed, empowered, safe and confident in using online technologies;
- Our businesses are resilient and can trade and prosper securely online;
- We all have confidence in the resilience of our digital public services.

4.2 In addition 4 key objectives have been identified in order for Scotland to become more cyber resilient:

- Provide effective leadership and promote collaboration
- Raise awareness and ensure effective communication
- Develop education and skills in cyber resilience
- Strengthen research and innovation

4.3 A draft response is presented for approval and is attached at Appendix 1. It welcomes the proposed strategy and suggests that it should be developed to add an additional focus on preventing and detecting cyber crime in Scotland, and that the strategy is linked more strongly to the UK Government's "UK Cyber Security Strategy". It also suggests mandating the Public Service Network across the Scottish public services to allow for more consistent and greater protection for citizens' personal data.

5.0 CONCLUSIONS

5.1 Policy and Resources Committee is asked to approve the draft response attached at Appendix 1.

6.0 IMPLICATIONS

6.1	Policy:	Affects all citizens and businesses in Scotland.
6.2	Financial:	Scottish Government will need to provide funding for any new or changed public sector actions that flow from the detailed action plan that will follow.
6.3	Legal:	New legislation is not anticipated.
6.4	HR:	None.
6.5	Equalities:	Changes will need to be subject to an equalities impact assessment at a national level.
6.6	Risk:	The strategy is intended to reduce risks.
6.7	Customer Service:	If implemented well, this will assist the council's Digital First policy and encourage customers to transact more online.

Appendices

1 Draft response to consultation questions

Douglas Hendry
Executive Director Customer Services
17 July 2015

Policy Lead: Councillor Dick Walsh

For further information please contact Judy Orr, Head of Customer and Support Services Tel 01586-555280 or Gerry Wilson, ICT and Digital Manager, Tel 01436 658936

Appendix 1:
Annex B
Cyber Resilience Strategy

The Scottish Government
Riaghaltas na h-Alba

RESPONDENT INFORMATION FORM

Please Note this form **must** be returned with your response to ensure that we handle your response appropriately

1. Name/Organisation

Organisation Name

Argyll and Bute Council

Title **Mr** ☒ **Ms** ☐ **Mrs** ☐ **Miss** ☐ **Dr** ☐ ***Please tick as appropriate***

Surname

Wilson

Forename

Gerry

2. Postal Address

Kilmory		
Lochgilphead		
Postcode PA31 8RT	**Phone** 01436 658936	**Email** gerry.wilson@argyll-

***3. Permissions* - I am responding as…**

Individual ☐ / **Group/Organisation** ☒

Please tick as appropriate

(a) Do you agree to your response being made available to the public (in Scottish Government library and/or on the Scottish Government web site)?

Please tick as appropriate ☒ **Yes** ☐ **No**

(b) Where confidentiality is not requested, we will make your responses available to the public on the following basis

Please tick ONE of the following boxes

Yes, make my response, name and address all available ☐

or

Yes, make my response available, but not my name and address ☒

or

Yes, make my response and name available, but not my address ☐

(c) The name and address of your organisation ***will be*** made available to the public (in the Scottish Government library and/or on the Scottish Government web site).

Are you content for your ***response*** to be made available?

Please tick as appropriate ☒ **Yes** ☐ **No**

(d) We will share your response internally with other Scottish Government policy teams who may be addressing the issues you discuss. They may wish to contact you again in the future, but we require your permission to do so. Are you content for Scottish Government to contact you again in relation to this consultation exercise?

Please tick as appropriate ☒ **Yes** ☐ **No**

CONSULTATION QUESTIONS

National leadership; Shared responsibilities; Working together; Protecting Scotland's values

Q1 Are the guiding principles right for this strategy?

Yes ☒ No ☐

Are there any other principles that should be considered when continuing to develop the strategy?

Yes. The other principle which should be considered is one of "tackling cyber crime in order to create an effective deterrent."

We consider that the principle of "Working together" to be particularly important. At present, we do not do this effectively across the public sector or the other parts of Scotland's society. The Public Service Network (PSN) was designed as a first step to the introduction of a more secure means of sharing information across the UK Public Sector. It bypasses the dangers of the Internet and offers a higher level of protection to the systems and data we operate and own. At the moment we are finding it increasingly difficult to work together with other public sector partners because of the complexities of the PSN, the different ways the standards have been applied, and the lack of a standard approach to Cyber Security and PSN accreditation between local authorities and the NHS. The Scottish Government can play a key role to facilitate such partnerships by ensuring individual public sector organisations all meet the same cyber security standards.

This would be particularly beneficial in helping to integrate Health and Social Care partnerships which at present is made more difficult by a lack of consistent approach regarding the PSN.

Our vision is for a cyber resilient Scotland that is safe, secure and prosperous

Q2 Do you agree with the vision?

Yes ☒ No ☐

Strategic Outcomes:
1. Our citizens are informed, empowered, safe and confident in using online technologies
2. Our businesses are resilient and can trade and prosper securely online
3. We all have confidence in the resilience of our digital public services

Q3 Do you agree with the strategic outcomes?

Yes ☒ No ☐

Are there additional outcomes that should be considered?

We agree with the vision but would welcome elements in the strategy which will make that vision deliverable, as we see this as very challenging. Without full control of all of the systems and software which we use to manage information we can never be 100% confident that all of Scotland will be "cyber resilient", or everyone will operate in a "safe, secure and prosperous" environment.

We have a duty and responsibility to protect citizens from the dangers of cyber crime and we all need to be confident that the private and public sectors have taken all necessary steps to protect systems and data. Vulnerable groups are continually threatened by nuisance callers or by those who steal identities and cash from bank accounts and this tells us we are far from such a Utopia. We allow such transactions to go undetected. We allow

rogue businesses to operate on our telephone networks and perpetrate the crimes.

We would welcome an additional outcome focussed on prevention and on the tackling of cyber crime, building on the UK Government's Cyber Security Strategy and showing how the Scottish Government is supporting this and implementing key deterrents in Scotland.

Key Objectives:

1. *Provide effective leadership and promote collaboration*
2. *Raise awareness and ensure effective communication*
3. *Develop education and skills in cyber resilience*
4. *Strengthen research and innovation*

Q4 Do you think these are the right objectives to focus on?

Yes ☐ No ☒

Are there additional key objectives that should be considered?

We have in our powers the ability to control the traffic on our networks, block access to the most dangerous parts of the Internet, block calls from foreign call centres, etc. Leadership, Communication, Education and Innovation is not enough - we must offer some kind of national protection which would make it difficult for those who currently perpetuate cyber crimes with relative impunity. We appreciate the complexities in finding a balance between an open society and the rule of law. The most effective way to manage these risks in through investment in prevention and this will also include effective tackling of cyber crimes. We suggest an additional objective of having the skills to tackle cyber crime and actively doing this.

Objective 1: Provide effective leadership and promote collaboration

Main areas of focus:

- *The Scottish Government to set up and lead a national strategic implementation group to implement, monitor and evaluate the impact of this strategy*
- *The Scottish Government to be at the forefront of providing safe and secure services, and sharing their knowledge with other organisations*
- *Collaborating with partners, the Scottish Government will lead and coordinate efforts to develop national cyber resilience*
- *Ministers and their officials continue to raise the profile of the importance of cyber resilience across a range of policy areas*
- *Ministers report on the Government's progress in building a culture of cyber resilience and good practice across the Scottish Government and its agencies*
- *The standards of cyber resilience adopted by the Scottish Government's on-line services – and those of other public agencies - will be available to service users.*

Q5 Do you agree with the main areas of focus for effective leadership and collaboration?

Yes ☒ No ☐

Are there other areas that should be considered?

Mandating standards across the Scottish public sector will at least tackle the problems we now face in joining disparate systems and organisations together.

It would also be helpful if there were a firm commitment to work closely with the UK Government on this topic and actively support the UK Cyber Security Strategy.

Objective 2: Raise awareness and ensure effective communication

Main areas of focus:

- *The Scottish Government alongside its partners to co-ordinate general awareness raising activity to promote a culture of cyber resilience among all Scottish citizens, including promoting the national online safety websites Get Safe Online and E-crime Scotland across Scotland*
- *Stakeholders and partners to implement audience-specific awareness raising activity - targeted at employees, educators, leaders and board members*
- *Working alongside the UK Government, the Scottish Government and partners from across the business world to form a network to share information about online threats and vulnerabilities*
- *Industry professionals develop and promote best practice in cyber resilience*

Q6 Do you agree with the main areas of focus for raising awareness and ensure effective communication?

Yes ☒ No ☐

Are there other areas that should be considered?

The GetSafeOnline site should be more heavily marketed. A Cyber Resilience strategy is only needed because the cyber threats are continuously increasing and current levels of awareness and protection are not high enough. We could go further with accreditation and go beyond the Information Assurance accreditation process for the PSN members only. Consideration could be given to a national accreditation scheme for businesses and organisations who can meet exacting standards of awareness and have adopted a cyber-resilient culture. This would in turn build confidence amongst customers that they are dealing with Cyber savvy organisations across all sectors in Scotland.

Objective 3: Develop education and skills in cyber resilience

Main areas of focus:

- *The Scottish Government and its partners promote the development and delivery of cyber resilience education in early learning and childcare settings, schools, colleges, universities and other learning settings*
- *Business partners build cyber resilience capabilities within workforces*
- *Scottish Enterprise and other business partners help develop the cyber security and resilience goods and services industry in Scotland*

Q7 Do you agree with the main areas of focus for developing education and skills in cyber resilience?

Yes ☒ No ☐

Are there other areas that should be considered?

We should also extend the PSN accreditation and further develop an accredited British Kite Mark standard such as the e-trader standard for online businesses which would identify organisations where all relevant staff have been trained to meet a particular cyber resilience standard, and where the organisation's management of core data also meets an agreed standard.

Objective 4: Strengthen research and innovation

Main areas of focus:

- *The Scottish Government, Police Scotland and partners progress with research to baseline the cost of cybercrime to Scotland*
- *Partners undertake and share research on understanding "what works" in preventing cybercrime, using knowledge from local, national and international angles*
- *Partners work together to target funding for cyber resilience research*
- *Enterprise funding is targeted at innovative methods to support the cyber resilience of individual or groups of enterprises*

Q8 Do you agree with the main areas of focus for strengthening research and innovation?

Yes ☒ No ☐

Are there other areas that should be considered?

It might be possible to extract a subset of the data used by the UK Government in baselining their strategy for Cyber Security.

How will we use the strategy to achieve real change?

For each of the outcomes, the Scottish Government and its partners are developing a detailed action plan setting out the short, medium and long term activities. These specific measures will be published in early 2016. Within this action plan there will be practical activities, projects and improvements to support individuals and organisations to become more cyber resilient, as well as steps to build up the cyber security goods and services sector in Scotland.

Q9 Are there additional actions that will help us achieve making Scotland and its people more cyber resilient?

The Scottish Government could mandate the use of the PSN for all public sector online activity and ensure that all known vulnerabilities in public sector networks are managed on a risk based approach. A similar approach could be encouraged within the private sector.

How will we know if we are succeeding?

The Scottish Government will be asking stakeholders to share their action plans and keep track of milestones and progress on an annual basis. This will help to provide regular annual updates to the national strategic implementation group.

Q10 Do you think the monitoring and evaluation arrangements are sufficient?

Yes ☐ No ☒

If not, what arrangements would you like to see?

The proposed monitoring and evaluation arrangements would represent a significant step forward. However we are concerned that in an open market, where cloud based systems and applications are hosted anywhere in the world, that it will be difficult to give any guarantees to the general public that the systems they rely upon are safe and secure. It is not possible to hold global online organisations to account under different legislative frameworks. If we want to offer our customers such assurances, we must stop the illegal activity. Education and awareness may help but it will not stop cyber related crime or eradicate the threats, and the latter is essential in building public confidence in operating online.

Q11 Have you ever experienced cyber crime (see examples on page 16)?

Yes ☐ No ☐

If so, did you report it? Please provide details.

Q12 Would you be willing to share your experiences with us?

Yes ☐ No ☐