Economy

Consultation copy -July 2025

Draft: for consultation purposes only

DRAFT Cyber Security Policy Framework 2025-2040

Raising Jersey's cyber resilience

Contents

Introduction

Purpose of the Policy Framework

The Cyber Security Policy Framework sets out the policy ambitions for Jersey to:

1. Empower Islanders and businesses to thrive in a safe and trusted digital environment
2. Build a resilient digital ecosystem
3. Reduce the impact of cybercrime on Islanders
4. Build upon opportunities in the area of cybersecurity that support economic growth

Background

Jersey's ambition to become a high performing, sustainable and technologically advanced economy by 2040[1] is dependent on establishing and maintaining a secure and trusted digital ecosystem.

Financial services currently contribute 40% of the Island's economic activity, meaning the Island is a more attractive target for cyber attacks than jurisdictions with a less financially sophisticated profile. Along with threatening Islanders' wellbeing, a major cyber attack could cause severe reputational and financial damage and serious harm to our economy.

This Cyber Security Policy Framework builds upon the work of Jersey's first Cyber Security Strategy[2], which raised awareness of the Island's vulnerabilities and the need for collective action. Central to delivery of the first strategy was the creation of a technical centre of cyber security excellence, to support businesses and Islanders, share intelligence and help defend the Island against cyber threats.

The Jersey Cyber Security Centre (JCSC) is now operational and has become a full member of the global Forum of Incident Response and Security Teams (FIRST) and an accredited member of the Task Force Computer Security Incident Responses Teams (TF-CSIRT). The proposed Cyber Security (Jersey) Law 202- will formalise its role in co-ordinating cybersecurity intelligence and promoting good cybersecurity practice for the Island and place duties on Operators of Essential Services to improve the Island's cyber resilience.

Islanders must be able to rely on the digital services they access. As digital services expand, so do public expectations for safety and data protection. As emphasised in the Government's Digital Economy Framework, digital growth must be underpinned by confidence in cyber security.

Cyber threats are escalating in scale and sophistication. Jersey is not immune. Investing in cyber security is essential. The technology to exploit vulnerabilities is evolving more rapidly than the security safeguards with many reports that cybercrime is now a $10 trillion industry, affecting businesses, organisations and individuals.

[1] See Strategy for Sustainable Economic Development
[2] See C Cyber Security Strategy 20170215 VP.pdf (gov.je).

In 2024 alone, Islanders lost over £2.5 million[3] to digital scams and the World Economic Forum[4] highlights supply chain vulnerabilities as the biggest barrier for achieving cyber resilience. AI has helped criminals to automate vulnerability scanning and create sophisticated phishing campaigns, capitalising on digital transformations faster than businesses are responding.

Lack of cyber awareness and under investment in cyber security is ultimately a cost borne by society. An Island-wide culture change is needed. Jersey must embrace "*secure by design*" and "*zero trust*" concepts. Across the business community, too many small businesses consider cyber security as an IT expense rather than a business investment and Directors must embed cyber resilience into corporate governance and actively manage cyber risks.

Just as technology and behaviours in this area are evolving, government policy needs to keep pace and anticipate future challenges and cyber threats. Government has an important role to play, setting expectations and raising standards. Government's commitment to securing trust in Jersey's digital infrastructure is reflected in the recent amendments to the Telecommunications (Jersey) Law 2002 and government investment in its own digital infrastructure to deliver secure digital services.

[3] See JCSC Confirms New Cryptocurrency Scams Part Of Ongoing Campaign | Jersey Cyber Security Centre
[4] See WEF_Global_Cybersecurity_Outlook_2025.pdf, published January 2025

Vision and Goals

Strong cyber security is seen as an *economic enabler* which can build and retain trust across the economy. In turn this will boost competitiveness, encourage digital innovation, drive productivity and reduce loss caused by cybercrime. This Cyber Security Policy Framework supports the Island's sustainable economic growth vision[5] for 2040 through a holistic and collaborative approach.

Vision

The vison of the Cyber Security Policy Framework is focused on:

Optimising Jersey's cyber security and cyber resilience, enabling Islanders and businesses to prosper

Overarching policy goals are:

- To advance awareness of cyber risks and the adoption of cyber security best practice Island-wide and to combat cybercrime through improved cyber resilience;
- To foster a safe and trusted digital ecosystem, underpinned by secure digital infrastructure and expertise in cyber skills; and
- To engage in thriving partnerships that support local cyber industry, and encourage investment and activity in cyber security services and design to support economic growth.

Alignment to critical Island interests:

[*DIAGRAM TO BE DEVELOPED AND ADDED POST CONSULTATION*]

[5] See: Strategy for Sustainable Economic Development, published October 2023: R-158-2023.pdf

Our Strategic Priorities

To achieve the vision of this Cyber Policy Framework, focused delivery will be measured against the following five strategic priorities:

1. **Strengthening cyber security within businesses, organisations, and for Islanders:** *We will ensure businesses, organisations, and Islanders understand the cyber threats they face, supporting them having in place relevant protective measures and their recovery from a cyber attack.*

2. **Continual development of an Island-wide resilient digital ecosystem:** *We will foster strategic partnerships to protect our digital data, shape future policy, develop appropriate legislative and regulatory frameworks and support economic growth.*

3. **Growing cyber security skills and capabilities:** *We will invest in growing cyber security skills and career pathways, deepening partnerships between government and industry.*

4. **Responding to the rise in cybercrime:** *We will ensure Jersey is prepared for and able to disrupt and combat cybercrimes affecting Islanders.*

5. **Building a thriving cyber industry:** *We will leverage a skilled, professional and diverse workforce to take full advantage of economic opportunities to grow a strong local cyber industry.*

Each of the above strategic priorities are explored in more detail in the following pages. For each strategic priority, the policy ambitions, priorities and current challenges Jersey needs to address are set out, along with the key delivery objectives.

A supporting Action Plan is to be published with input from key delivery partners and stakeholders. The Action Plan will:

- Uphold our commitment to meet our policy ambition through a collaborative and holistic approach
- Identify the initiatives to be achieved and delivered in the short-, medium- and long term
- Set out detailed measurement of success.

Strategic Partnerships

Strategic partnerships are instrumental in enabling Jersey to raise its cyber resilience Island-wide in line with this policy framework.

The digital ecosystem is complex. We all play a vital role. Only by working together as a community, from boardrooms to classrooms, can we build a robust defence against cyber threats and protect our collective digital well-being. As an Island, we are increasingly reliant on the digital environment in our business, social and personal interactions. In order to benefit fully from our digital transformation, we must be able to trust in the security of our digital ecosystem; remain confident in data management and uphold the protection of users' rights and interests.

Key strategic partnerships include, but are not limited to:

Jersey Cyber Security Centre (JCSC): Providing technical expertise to help the Island "*prepare for, protect against, and respond to*" cyber attacks, the JCSC is instrumental to Jersey being "*internationally recognised as a safe place to live and do business online."* JCSC acts as Jersey's gateway into international cyber emergency response networks, giving the Island access to the latest cyber intelligence and expertise, helping to detect vulnerabilities and promoting a culture of cyber security information sharing and vulnerability management.

Law enforcement: As the technical ability of bad actors increases, it must be matched by the technical ability of those with a legal duty to protect. Jersey has established the Financial Intelligence Unit, the Economic Crime and Confiscation Unit, the Joint Financial Crime Unit and the Jersey Fraud Prevention Forum, all working together alongside the States of Jersey Police to combat cybercrime and protect Islanders. Digital crimes do not respect geographical or international boundaries. It is more important than ever for these agencies continue to work in close collaboration with their key partners off-Island and forge new relationships where necessary.

Regulatory bodies: Jersey regulators have their part to play, whether it is in ensuring Islanders' personal data is kept safe, regulating cyber secure business practice or promoting the highest security standards from our telecommunication providers. The Island looks to regulatory bodies, such as Jersey Data Protection Authority, Jersey Financial Services Commission and Jersey Competition Regulatory Authority and their international regulatory networks, to provide thought leadership and ensure Jersey is adequately informed to take advantage of new technologies and employ responsible business practices.

Business communities: Jersey business leaders need the skills, tools and knowledge to lead their teams and businesses through the necessary digital transformations over the coming years. A cyber resilient culture must be embedded that flows through from their board rooms into their supply chains, providing necessary reassurance to clients. Jersey Institute of Directors, Jersey Chamber of Commerce, Jersey Finance and the Channel Islands Information Security Forum have key roles in championing culture change, raising awareness of cyber security risk management and advocating for development of relevant skills within our Island's workforce.

Operators of Essential Services: These entities include government services that provide critical services. We look to them to show leadership to the business community in enhancing their own cyber security risk management, reducing their cyber risk profile and meeting best

practice and sector-specific cyber security standards. A significant cyber attack suffered by any of them is a risk to Jersey's international reputation, our economy and Islanders' wellbeing.

International engagement: Despite its small size, Jersey is well connected. Our strong relationships with other leading jurisdictions mean that we can share best practices and intelligence, receive expert advice and leverage access to specialist intelligent resources. These relationships must be preserved and fostered to achieve the aims of this framework.

> "***cyber security is a shared responsibility*** *between the public and private sectors – everyone is involved – from governments, critical infrastructure, corporations, small and medium-sized businesses, financial institutions, healthcare providers, service providers, employees, vendors, remote employees, and individuals.* "
>
> Brad Smith, Vice Chair and President at Microsoft Corporation

Strategic priority 1: Strengthening cyber security within businesses, organisations and for Islanders

We will ensure businesses, organisations, and Islanders understand the cyber threats they face and support them putting in place relevant protective measures and recovering from a cyber attack.

Background

In excess of 8,200 businesses are registered in Jersey, of which 89% have fewer than 10 full-time employees[6].

Thriving small businesses are important to Jersey's economic future. Many do not have dedicated IT staff, let alone a security team. These small businesses, individual Islanders and other entities need help to engage the right professional help procure the right services. A cyber incident can be costly and potentially devastating for them.

The cyber risk profile of the digital estate of larger businesses, organisations and Government is much higher. Continuity of service is heavily reliant on the cyber security of their supply chain. Despite this, Islanders rely on them to deliver critical and essential services.

Navigating available cyber advice and understanding the appropriate level cyber security that should be sought can be challenging in all parts of the community. Trusted answers to questions like: '*What does good cyber security look like?*' and '*What cyber security measures are appropriate for me/my business*?' can be hard to find.

Policy ambition

For every business, organisation and Islander to have the necessary skills and resources to be cyber secure by 2040.

This will enable Jersey to benefit from a strong digital economy where businesses, organisations and Islanders routinely use digital environments without fear to boost productivity, access services and within their daily lives.

For a mutually supportive and cyber security aware community to have been established Island-wide where everyone understands the role they play.

A culture where Islanders work together to continue to raise the cyber security of the Island and all know how to get help quicky to reduce the impact of cyber attacks.

From board members to business owners, charities to individuals, cyber will have progressed from a topic discussed purely within cyber professional networks to an everyday appreciation of how to manage risks. Whether an entity is operating as part of the Island's critical infrastructure, or is a micro-business, the appropriate level of cyber security is embedded.

For the role of the Jersey Cyber Security Centre (JCSC) as the Island's cyber technical advisory body to be embedded within the community Island-wide, with advice and guidance routinely sought from, and provided by, JCSC.

[6] Jersey Business, 2023 Annual Report (p22) jbl-annual-report-accounts-2023.pdf

The JCSC to have the resources and capabilities to provide a 24/7 support service to businesses and Islanders.

Islanders and businesses to routinely seek technical advice to help reduce the risk and impact of cyber incidents. The sharing of cyber incident information in a timely fashion is routine, reducing vulnerabilities and increasing resilience.

The JCSC to excel at providing threat information to essential services that is received and acted on. Likewise, threat information to be routinely shared with JCSC, enabling appropriate Island-wide action to be taken to mitigate any rising cyber risks.

The JCSC to offer a suite of tools applicable to the size and scale of our local business, helping reduce their vulnerabilities and deliver secure services, including advice on how to identify reputable cyber security providers and products. Local businesses to routinely access and trust such tools and JCSC's services, such as the Jersey Cyber Shield.

For customer trust and business reputations to be upheld by the implementation of relevant best practice cyber security standards.

Cyber incident management processes in all businesses, irrespective of size, to be routinely tested and refined. Key digital assets to be identified; contingency plans to be routinely tested and zero trust protocols adopted.

Customer trust and business reputations to be upheld by the implementation of relevant best-practice cyber security standards. Advice and guidance are routinely sought and provided by JCSC.

The Government of Jersey to lead by example, maintaining and routinely improving cyber security across its digital estate, protecting the confidentiality, integrity and availability of critical digital government data, and providing trusted digital services for Islanders.

Challenges

A culture of associating the reporting of cyber incidents with regulatory requirements and a sense of 'failure' - rather than good ethical practice - needs to be overcome.

Challenging this perspective will enable businesses to routinely and confidently share cyber incident information with JCSC, as well as relevant regulatory bodies. This, in turn, will enable affected businesses to receive advice, support and guidance to help them recover effectively from incidents. In addition, sharing of cyber incident information will mean actions can be taken to raise awareness and promote good cyber hygiene.

Establishing a deeper understanding of cyber security opportunities and risks where companies make strategic decisions.

Company boards have an essential role in fostering a culture of strong corporate cyber security governance. Too often boards overestimate their company's cyber security preparedness[7].

Across the private sector and government, deepening cyber security understanding at a corporate level could transform the delivery of trusted e-services for us all. A

[7] See Boards Need a More Active Approach to Cybersecurity, published May 2025

greater understanding of the impacts, benefits or risks of cyber security on service delivery will ensure strategic development in cyber security capabilities are routinely addressed.

Clarity and trusted advice and access to up-to-date guidance would enable businesses to put the relevant measures in place and ensure they remain appropriate, irrespective of industry size or economic sector. The Jersey Cyber Security Centre (JCSC) is establishing its role in this space.

As JCSC becomes established and grows its reputation as the centre of expertise on cyber security, wider engagement regarding recommendations for appropriate cyber security standards for businesses will be supported.

Trust and understanding of advancing technologies and how they are safely incorporated into new tools and services needs to be built over time.

With no internationally recognised cyber security product safety standards or "*kitemark*", 'security by design' principles need to be adapted and adopted as a minimum to reassure customers and end users.

Implementation

- **We will continue to ensure development and delivery of co-ordinated cyber security awareness campaigns concentrating on risks, threats and ways to address them. These will be led by JCSC and delivered with support from government in the following way:**
  - JCSC to maintain and drive a co-ordinated and varied programme, which is developed in consultation with stakeholders and is supported by a clear implementation plan that has engagement and delivery support from relevant bodies
  - Joint awareness-raising efforts and collaboration across public-private initiatives to be realised and routinely assessed for effectiveness and support the delivery of the co-ordinated programme.
  - Best practice to be shared and resources pooled to ensure learnings are acted upon and are used to develop revised awareness campaigns.
  - Public authorities to co-ordinate, publish and inform users about privacy and security initiatives and lessons learned from breaches
  - A wide range of exercises, communication channels, events and tools to be used to promote awareness and measure impact of campaigns

- **We will ensure executives from the public, private and civil society sectors and especially Operators of Essential Services address cyber security risks in their organisations, including:**
  - Strategic assets to be identified and measures put in place to protect them
  - The mechanisms to protect strategic assets to be put in place, routinely tested and supported by contingency plans
  - Strategic direction and development to be underpinned by robust cyber security risk management

- **We will work towards an agreed baseline of cyber security related standards and good practices being identified that are appropriate and proportionate to Jersey businesses, reflecting their size and operational**

significance for the Island, including a balance of risk exposure, likelihood of occurrence and severity (including societal and economic impact) have been considered
    - Guidance to be available and accessible from JCSC to support businesses to achieve the relevant cyber security standards and good practice
    - A coordinated regulatory approach for cyber security has been established across Jersey's regulatory bodies to effectively monitor compliance

- **We will encourage cyber incidents to be shared with JCSC as a matter of routine, promoting a culture of information sharing**
    - Operators of Essential Services to routinely report significant cyber incidents within 24 hours to JCSC
    - JCSC to routinely review reported incidents and responds accordingly depending on the recognised category of severity
    - Businesses and organisations to have established internal mechanisms for identifying and categorising cyber security incidents which are routinely reviewed and updated
    - Non-significant incidents to also be routinely shared with JCSC, to raise resilience and reduce impact for all
- **We will ensure incident response is co-ordinated across key Island responding agencies**
    - the roles of JCSC, Government Digital Services, States of Jersey Police, Government Emergency Response and Resilience teams and other bodies, like Jersey Regulators, will be established, understood and supported by relevant Memoranda of Understanding
    - Learnings from incidents will be captured as a matter of routine and shared without commercial compromise or reputational stigma
    - Island-wide cyber security incident exercises will be regularly held covering a range of cyber security related scenarios, with lessons learned being routinely embedded and enforced
    - Emergency communication systems will be regularly tested for cyber resilience
    - Off-island dependencies to be identified and routinely tested for cyber resilience

- **We will ensure threat intelligence and vulnerability is routinely collated by JCSC and shared with relevant Jersey organisations**
    - JCSC will have built good collaborative relationships with relevant partners both on- and off-island
    - Jersey businesses will have embedded good operational practices to ensure appropriate action is being taken based on the vulnerability information received

Strategic priority 2: Continual development of an Island-wide resilient digital ecosystem

We will foster strategic partnerships to protect our digital data, shape future policy, develop appropriate legislative and regulatory frameworks and support economic growth.

Background

Cyber resilience can be defined as the ability of an entity to protect itself, detect, respond to and recover from cyber-attacks. Like cyber security, cyber resilience is foundational to protect our digital ecosystem and enable all to confidently take advantage of current and future digital technologies.

Jersey's security legislative environment needs to continue to evolve to remain current. The recent Telecommunication Regulation amendments and proposed Cyber Security (Jersey) Law 202- work alongside established legislative and regulatory frameworks. Their benefits will take time to be recognised. A number of respected jurisdictions have passed additional online safety and cyber security focused laws, which could benefit the Island if appropriately adapted and adopted.

Having been established as the Island's expert cyber technical advisory body, the Jersey Cyber Security Centre (JCSC) needs to develop its reputation as a respected centre of excellence over time.

Policy ambition

By 2040, for Jersey to have developed an effective whole Island approach, where every business, organisation and Islander takes responsibility and proportionate measures to underpin and maintain the Island's cyber resilience.

Improving our cyber resilience can only be achieved by working together.

For Jersey's operators of critical infrastructure and essential services to have evolved their resilience and capabilities to withstand and recover from cyber attacks.

This will require long-term investment and appropriate cyber risk mitigation plans and governance are embedded in everyday operations, providing the reassurance to Islanders that services they rely on every day are protected.

Irrespective of the size of business, cyber resilience testing to have become routine with lessons learned actioned and shared.

For cyber risks to be routinely mapped, discussed and mitigated with appropriate and proportionate technical, operational and organisational measures being taken.

For Government and business to understand the cyber risks of their supply chains and the impact of upstream disruption on the continuity of the service they provide to Islanders.

When procuring services, for Government and business to routinely request and consider minimum cyber standards as part of the procurement process and ongoing assessment of delivery.

For Jersey to have adapted and adopted international best practice into legislation and regulation to improve cyber resilience through minimising the impacts of cyber incidents.

This includes recommending technical and organisation measures, mandating cyber incident information sharing and strengthening the accountability of Boards of Directors and third-party service providers (TPSPs). This is to be done through a balanced approach to ensure legislation and regulation does not become burdensome and restrictive for economic development.

Further, for the Island's regulatory environment to be seamlessly aligned: duplication of reporting cyber incidents is minimised and sharing of information is maximised. As emerging technologies provide innovation opportunities, regulatory thought leadership should provide reassurance that cyber security standards are upheld, with Islanders being reassured that they can navigate the digital ecosystem with confidence and safety.

Jersey has previously embraced local legislative and regulatory changes and challenges to establish a proportionate data protection regime. This has ensured businesses can continue to operate internationally. This level of Ministerial ambition should be retained for building cyber resilience so that the Island can safeguard its international reputation, and economic standing.

For Islanders to understand how to protect their own data and to be reassured that their data is being protected.

Islanders to have confidence interacting with Government and local business through digital environments, and in accessing digital services.

For public and private sector investment to be maintained at a sufficient level to ensure a secure digital ecosystem for Islanders.

Challenges

Cyber threats may feel 'invisible'.

The interconnectivity of our digital world and our increasing reliance on digital solutions for day-to-day activities mean we all have a role to play to improve Jersey's cyber resilience. Rapid advancements in technology and the growth in online services and users requires ever evolving solutions.

Jersey needs to continue to invest to protect its critical infrastructure and Operators of Essential Services, the information that flows through them and the services they provide.

Improved cyber resilience will only be achieved by working together, across all of the Island's Operators of Essential Services, to share best practice and enhance cyber governance and to hold each other to account.

Jersey needs to keep pace with international advances in legislation and regulation for improved cyber resilience to avoid being considered an economic cyber risk.

Jersey has previously embraced local legislative and regulatory changes and challenges to establish a proportionate data protection regime. This has ensured businesses can continue to operate internationally. This level of Ministerial ambition should be retained for building cyber resilience so that the Island can safeguard its international reputation and economic standing.

Each regulatory body in Jersey considers the cyber security of the entities they regulate to be critical and are key partners to help raise cyber security standards and resilience. Building on the profile of local regulatory networks will help to proactively shape the future of Jersey's regulatory

environment and how this environment should respond to fast-paced changes in access and utilisation of digital technologies.

Cyber incidents need to be reported to multiple bodies or regulators.

The regulatory and reporting requirements for cyber incidents serve an important purpose but can be daunting when a business is responding to a cyber incident and needs to report to multiple bodies.

In addition, clarity on recommended cyber security standards for non-regulated industries would establish a clear direction for cyber security resilience that business can unite behind.

Jersey needs to maximise its international relationships to drive change, as technology changes at pace.

Jersey is small but can capitalise on its international relationships, whether built through Government, regulatory bodies or centres of expertise. This will bring best practice and thought leadership to the Island, from ensuring safe use of innovative technologies to sharing threat intelligence. Such relationships are key, where resource is constrained to develop it firsthand.

Jersey needs to carefully consider how data protection, online safety and cyber security are developed in harmony, to achieve the desired policy aims without constricting business development

A trusted and reliable digital ecosystem brings together these three key digital policy areas: data protection, online safety and cyber security. Only by working together with key strategic partners will we avoid duplication and enhance the final policy outcome, that protects Islanders but supports economic development.

The right level of public and private investment in cyber security is hard to quantify but is vital for success. The Government Budget[8] has many pressures on it.

Government must continue to invest in both internal cyber security and resilience programs as well as supporting strategic delivery projects and public-private partnerships need to become more widespread to help improve the Island's cyber resilience.

Implementation

- **We will ensure Jersey-based regulatory bodies help shape future digital policy, by:**
  - Continual review of the regulatory landscape to remove barriers and promote reporting, enabling businesses and Islanders to become more digitally secure, cyber resilient and confident in operating online, in a proportionate and agile regulatory environment.
  - Providing expertise, thought leadership and advice to help shape future digital and cyber security policy and regulations, enabling Jersey to prosper in a rapidly changing digital ecosystem and to capitalise on technological advancements without fear.
  - Routinely sharing lessons learned and good practice without compromising cyber security or confidentiality
  - Leading public debates addressing need to balance digital security and privacy

[8] See: Proposed Budget (Government Plan) 2025 - 2028P.51-2024-(re-issue).pdf

- **We will encourage supply chain resilience to be actively and routinely managed in all businesses, with Operators of Essential Services leading by example:**
  - Cyber security standards and best practices in guiding procurement process to have been developed and agreed with key stakeholders and include consideration of risk management, life cycle management software and hardware assurance, outsourcing, and use of cloud services
  - Guidance for implementation of procurement standards and best practices to have been developed by and are available from JCSC
  - Procurement process developed by Government and Operators of Essential Services highlight and endorse best practice, and learnings to be routinely shared for continuous improvement
  - Cyber resilience exercises to be routinely held by Operators of Essential services which involve their key supply chain partners, irrespective of whether they are based on Jersey or not

- **We will leverage our International collaboration to highlight specialist cyber security capabilities that Jersey can rely on, including**
  - established collaborative partnership with the UK's National Cyber Security Centre with JCSC and Government
  - JCSC representing Jesey's cyber security interests in key international forum and develops collaborative partnerships. Through these networks, JCSC will leverage cyber security thought leadership, bringing initiatives on island where impact can be measured

- **We will ensure co-ordinated cyber security awareness campaigns across multiple agencies, supporting widespread awareness of cyber security risks within government, private firms and amongst Islanders.**

- **We will ensure that, as the cyber threat landscape changes, government bodies and the private sector routinely follow safe cyber security practices and proactively take the necessary steps to improve cyber security, including:**
  - Ensure up-to-date technological security controls are deployed
  - Protection of data to international standards, whether at rest or in transit, with sector specific guidance available
  - Relevant technical security measures and controls deployed by both public and private sectors that reflect internationally established cyber security frameworks, standards and good practice, with sector specific guidance available

- **We will continue to evolve data protection, cyber security, online safety and telecoms security legislative and regulative frameworks to protect Islanders.** This will be achieved through cross-sector collaboration to:
  - continually review the impact of local legislative and regulatory frameworks and address gaps
  - develop local legislation to ensure evolving Operators of Essential Services are captured
  - assess impact of global changes in cyber, data protection and digital

safety legislation and regulation to adapt and adopt as necessary

- **We will ensure government invests in cyber security initiatives appropriately alongside public-private funded projects to raise the Island's cyber resilience.**

Strategic priority 3: Growing cybersecurity skills and capabilities

We will invest in growing cyber security skills and career pathways, deepening partnerships between government and industry.

Background

The World Economic Forum identifies[9] digital and technology skills including AI, big data, computer networks and cyber security as critical for the future job market.

Policy ambition

For Jersey to have established by 2040 a robust pipeline of cyber security talent, ensuring the Island's workforce is equipped with essential cyber and technology skills.

The 2017 Cyber Security Strategy ambition to "*Educate for the future*" remains just as valid today.

Strong, mutually beneficial partnerships between private companies, secondary schools, Highlands College and higher education institutions will drive hands-on experience and internships, fostering early career interest and practical skills in cyber security. Private companies will actively invest in local cyber programs, providing financial support, industry expertise, resources and structured training programs that bridge the gap between education and employment.

Cyber security professionals on the Island will have clearly defined professional recognition and continuous professional development opportunities.

Regular training and certification will ensure professionals remain adept at identifying and managing evolving threats, such as deep fakes, through continuous skills updates and awareness campaigns.

Government will demonstrate leadership by mandating regular cyber security and data protection training for all public sector employees, elected officials and partners, reflecting a culture of robust cyber security awareness at every level.

Challenges

Ensuring Jersey has a sufficient pipeline of cyber security and digitally-savvy professionals.

Current levels of digital education funding in Jersey schools have not matched the rapid technological evolution, potentially resulting in inconsistencies and gaps in cybersecurity education delivery. Stronger cross-Ministerial prioritisation and coordinated implementation are required to support the aims of the Government's Digital Education Strategy[10] to close this gap.

Locally, the Channel Island Information Security Forum[11] (CIISF) has noted members find it difficult to attract and retain experienced cyber security professionals, with an acute gap within technical cyber security domains.

[9] See: WEF_Future_of_Jobs_Report_2025.pdf, published January 2025

[11] See: Channel Islands Information Security Forum (CIISF)

Funding challenges have put at risk the future availability of digital skill courses on offer through Digital Jersey's Digital Skills Academy.

Such courses have helped Islanders and businesses take advantage of new technical developments to improve productivity, innovate or grow.

Education leaders have identified the need for enhanced digital careers advice and stronger, practical links with the digital and technology sectors.

Jersey underutilises available UK resources, like the training materials developed by the UK's National Cyber Security Centre (NCSC) CyberFirst[12] program, which is designed to inspire and encourage students to consider a career in cyber security and offers structured frameworks for cyber security education.

Unlike sectors such as construction[13], Jersey's digital sector, including cyber security, currently lacks a centralised industry body to advocate effectively for policy development alongside skills promotion and professional standards. Locally, the CIISF facilitates professional training and are looking at how to support members to promote links with local education facilities.

Recognition and accreditation of cyber security professionals remains limited locally

Adopting standards from established bodies such as the UK Cyber Security Council[14] could offer clear benchmarks for skill levels, ensuring consistent, high-quality cyber security practices across the Island's workforce.

Implementation

- **We will actively encourage the private sector to establish an industry-led professional cyber security development body, or similar, to advocate for policy alignment, skills enhancement and industry-wide standards.**

- **We will establish routine career awareness initiatives supported by the private sector, including**
  - Leveraging Jersey Association for Digital Education (JADE) to expand student exposure to cyber security careers
  - Regular summer placements and internships from local businesses for secondary and tertiary students
  - Structured work experience opportunities through programs such as Trident
  - Active corporate social responsibility programs where local professionals engage directly with schools through programs like CyberFirst.

- **We will ensure comprehensive, ongoing training programs for cyber security professionals are available, supported by local businesses, highlighting clear pathways to Chartered status**

- **We will promote mandatory cyber security and data protection training**

[12] See Schools - NCSC.GOV.UK for Cyber First materials

[13] See Jersey Construction Council (JeCC) - The Heart of Jersey's Construction Community

[14] See the UK Cyber Security Council Cyber Security Professional Standards Specialism Roadmap at Specialism Roadmap

for all government and elected officials

Ensuring a strong cyber security culture permeates all levels of governance and service delivery

Strategic priority 4: Responding to the rise in cybercrime

We will ensure Jersey is prepared for and able to disrupt and combat cybercrimes affecting Islanders.

Background

As emerging technologies are rapidly adopted, cybercriminals are harnessing them just as effectively to exploit new vulnerabilities at a greater scale and level of sophistication.

Jersey is a small jurisdiction and develops strong international links to help fight cybercrime, a criminal activity that do not respect international boundaries. The States of Jersey Police's own Policing Plan[15] states their strategic ambitions, supported by strengthening cyber resilience.

The impact of ransomware on local businesses can be devastating and is becoming more accessible to bad actors due to 'ransomware-as-a-service' products being advertised for sale on the dark web.

Australia, which has had its national cyber security legislation in place for a number of years, is now consulting with businesses to establish a legal 'no-fault, no-liability ransomware reporting obligation[16]. Their ambition is to enable anonymised reports of ransomware and for cyber extortion trends to be shared, helping strengthen Australia's resilience to cybercrime and stop the payments that facilitate further criminal activity.

The Jersey Financial Services Commission (JFSC) has clear guidance on the purpose of the Island's Sanction Regime:[17] those that do pay ransoms to release valuable data may not be aware that they could be inadvertently breaking Jersey's current sanction measures.

Policy ambition

For cross-Ministerial support to increase the States of Jersey Police's (SoJP) capability and capacity to respond to evolving cybercrime.

A swift and efficient response to reported cybercrime for all Islanders is needed, that is co-ordinated across multiple agencies and jurisdictions.

This will be assisted by the SoJP championing the development of relevant technical skills within the multiple agencies tackling digital crime and digital financial crimes, with a focus on prevention rather than investigation. Information flows between all on- and off-Island law enforcement agencies, where collaboration is key to preventing cybercrime.

For Islanders to be aware of the evolving nature of cyber scams and have the confidence to report suspicious activity or seek help if needed and take active measures themselves to prevent being a victim of cybercrime.

Islanders to know where to report cybercrime and to be confident that help can be provided.

[15] See Policing Plan 2025- 2028

[16] See 2023-2030 Australian Cyber Security Strategy

[17] See Sanctions: Cyber-attacks — Jersey Financial Services Commission

Islanders to have the skills to protect themselves online and recognise non-legitimate internet sites and know how to validate information found online. A sense of 'zero-trust' is prevalent.

This will require the SoJP, Jersey Fraud Prevention Forum and Jersey Cyber Security Centre having a coordinated education and awareness programme to alert Islanders and businesses to the threat of evolving cyber scams. This to be based on the co-ordinated intelligence gathering of Island based financial crime agencies.

For Jersey's criminal laws and legislative framework to be regularly reviewed by multidisciplinary teams across government and the Island's financial crime agencies.

Updates to ensure criminal justice is served for cyber-related crimes. The interaction of legal frameworks between cyber security (technical aspects of security) and cybercrime (criminal justice response) to be properly considered, communicated and established.

Challenges

Almost all crimes committed today involve some level of digital forensic analysis. The sheer volume of digital evidence to be gathered and analysed and stored requires the appropriate resourcing, training and funding which is not currently the case.

The recent investment by SoJP of an extra £250,000 into their digital forensic unit is not currently keeping pace with cybercrimes as they grow in volume and sophistication. Continued investment is needed for software licences, hardware and training, to keep up with evolving digital developments and techniques.

A focus on prevention will benefit the community and SoJP resourcing. This would enable the most effective and efficient use of their digital forensics expertise, helping prevent cybercrimes or to speed up criminal proceedings and deliver timely justice for victims.

Jersey benefits from a very low general crime rate, creating a sense of complacency regarding security. The Island is not as readily protected from fraudulent, via digital means, activity targeting us in our homes, at work or on our mobile devices.

Unfortunately, many of these scams and frauds result in financial loss to Islanders.

Whilst there is an emphasis on educating Islanders against cybercrime within the Policing Plan, this focus will be more impactful if co-ordinated across more agencies.

There is a general under-reporting of these crimes, which creates a lack of understanding of the total impact of these crimes.

This in turn can lead to under-resourcing of skills and technology to protect Islanders.

Jersey is starting its own cyber security legislative journey, with the proposed Cyber Security (Jersey) Law 202- and therefore needs to develop confidence in Island-wide reporting of cyber incidences as a first step. Islanders need reassurance that businesses and government are keeping their data safe and secure now and in the future.

As technology and working practices change, Jersey needs to ensure its regulatory and legislative landscape protects Islander's data and privacy, enables a safe online environment and

ensures charges can be brought against digital criminal activity.

The rate of change of the nature of digital crimes is outpacing the change process of policy and legislation and amendments needed to improve conviction rates.

Legislative and regulatory developments can cut across many government departments and agencies with input needed from key stakeholders and experts.

The Violence Against Women and Girls Taskforce Report[18], made recommendations to strengthen the domestic legal framework to better protect Islanders against online and technology-facilitated abuse. Such targeted reviews with key experts and stakeholders can help Ministers prioritise legislative developments, but take time.

Globally, legislative and regulatory changes are happening to safeguard young people against online harms and ensure their data rights are protected. An appropriate and proportionate Island-wide response to online safety needs to be co-ordinated across Ministerial portfolios and incorporate the expertise of many stakeholders, including children themselves. The challenge is the pace of change failing to meet Islanders' expectations.

Implementation

- **We will ensure the roles and responsibilities of Jersey-based enforcement agencies are embedded, supported by relevant agreements and enforcement powers and understood by Islanders by:**
  - Co-ordination of awareness-raising campaigns to promote understanding of the scale, scope and impact of cyber related crimes
  - Campaigns providing targeted materials across all age groups to start building a culture of healthy scepticism when confronted with a cyber related material
  - Raising awareness of ongoing developments in cybercrime: this reduces the impact of such crimes on Islanders and improves reporting statistics so that the true scale and impact of these crimes can be properly mitigated

- **We will champion law enforcement agencies to be resourced to focus on digital crime prevention**
  This will include them having access to relevant training and equipment to operate in a changing and challenging digital law enforcement environment

- **We will continually review domestic legal frameworks against global changes and developments with involvement of key stakeholders**
  To:
  - Reflect changes that enable successful prosecution of tech-facilitated crimes
  - Ensure Islanders have confidence in the integrity and security of their digital data held by Government and other businesses
  - Ensure Jersey's cyber security and data protection legislative framework remain appropriate and proportionate
  - Enable Jersey's Regulatory bodies to apply suitable enforcement

[18] See Recommendations 11 and 12 VAWG Taskforce Summary Report.pdf

powers to ensure cyber security standards are met and ensure Islanders are afforded relevant protection and feel safe in a digital environment

- **We will deepen a collaborative approach through:**
  - Leveraging international cooperation, leading to better information-sharing across borders and agencies, and enhanced digital forensic capabilities
  - Shared information between all on-Island agencies with law enforcement capabilities, to avoid duplication and provide exceptional protection for Islanders
  - Shared information between on-island policy development, law enforcement and regulation bodies to highlight and address legislative gaps, regulatory challenges and policy hurdles
  - Work with new and established partners to raise the profile of Jersey and enable Jersey to proactively adapt in a challenging digital environment

- **We will continually review global response to ransomware to ensure Jersey remains a trusted jurisdiction in which to do business**

Strategic priority 5: Building a thriving cyber industry

We will leverage a skilled, professional and diverse workforce to take full advantage of economic opportunities to grow a strong local cyber industry.

Policy ambition

For Jersey to play a key role in future development of cyber security skills and products

Investment in cyber security skills and products to accelerate the development of next-generation security tools and business opportunities.

Innovation will be at the heart of this transformation, with emerging technologies nurtured, developed, and supported to create groundbreaking solutions. Companies will embrace advancements such as artificial intelligence, blockchain, and quantum computing, integrating them into cyber security frameworks to stay ahead of evolving threats.

Local economic development agencies will facilitate collaboration and provide safe sandbox testing environments.

A successful cyber industry will be built on the principle of 'secure by design', ensuring that security is embedded into products from their inception. This proactive approach will minimise vulnerabilities, making digital infrastructure more resilient and reducing the risks of cyber attacks. Security will be prioritised in software development, hardware design, and network architecture, reinforcing trust among consumers and within their business networks.

For a business-friendly environment to be fostered through supportive regulatory frameworks and strategic initiatives, while ensuring compliance with global cyber security standards.

Local regulatory authorities and industry and professional bodies will play a crucial role in shaping policies that support growth and remove barriers for local businesses. This will enable companies to navigate complex security requirements, while focusing on productivity growth, expansion and innovation.

For research and innovation partnerships with universities and key global industry players to be leveraged to solidify Jersey's local cyber security industry's foundation for long-term success.

These collaborations will drive advancements in cyber security, allowing businesses to access cutting-edge research, skilled graduates, and specialised expertise.

A thriving cyber industry will not only contribute to economic growth but also safeguard digital assets, reinforcing trust and confidence in an increasingly connected world. With diversity, innovation, security, policy support, and academic partnerships at its core, the growth of Jersey's cyber security industry will be well-positioned to support the economy and address the challenges of the digital age.

Challenges

Jersey faces several challenges in building a thriving cyber industry. One key issue is infrastructure limitations.

While Jersey has strong broadband connectivity, its public services—such as government IT systems, healthcare

technologies, and education lag behind in digital transformation. Without strong commitment and funding to modernise infrastructure, the Island may struggle to support the technological advancements needed for a robust cyber industry and growing digital economy.

Another challenge is cyber security preparedness.

The 2017 Cyber Security Strategy emphasised the need for a cyber-resilient island where businesses and individuals are well-informed about cyber risks. However, ensuring that all businesses prioritise cyber security and have the necessary resources to protect themselves remains a hurdle. As an island nation, security has not been a cultural priority. The Government aims to facilitate information sharing and set minimum security standards, but widespread adoption and compliance require significant effort.

Trust, and understanding of advancing technologies and how they are safely incorporated into new tools and services, needs to be built over time. With no internationally recognised cyber security product safety standards or "*kitemark*", 'security by design' principles need to be adapted and adopted as a minimum to reassure customers and end users.

Talent and skills development pose a challenge.

Impact Jersey[19] seeks to address skills gaps by funding technological solutions and supporting innovation. However, ensuring that Islanders have the right expertise for future cyber security demands is an ongoing concern. Without a well-educated workforce, businesses may struggle to find skilled professionals to drive innovation and security. The cost of island-living is also a key factor in keeping talent on-island.

Finally, economic and regulatory barriers can slow progress.

Jersey has a strong financial services sector, but it has yet to fully capitalise on fintech and cyber security opportunities. The Island's size and autonomy could be an advantage in creating agile regulatory frameworks, but Jersey must balance innovation with compliance to remain a trusted jurisdiction. Developing a fintech hub and fostering a business-friendly environment[20] will be a crucial first step for attracting investment and supporting local businesses and driving digital economic growth.

Overcoming these challenges will require coordinated efforts from Government, businesses and educational institutions both on and off the Island, to ensure Jersey can achieve its vision of a thriving cyber industry.

Implementation

- **We will seek opportunities for an alternative approach to policy development through recognised collaboration with neighbouring or similar jurisdictions to open up innovative opportunities and drive the pace of change beyond what Jersey can achieve on its own.**
    - Whilst Jersey has its own government-led policies we should also look to our close neighbours

[19] https://impact.je/

[20] The Challenges and Opportunities: How Jersey Can Become a Technologically Advanced Economy – Adapt Consulting Company, published 18 October 2024

and the network of Crown Dependencies to achieve more and quicker by leveraging aligned policy intent and ambition and uniting behind a common voice.
    - The JCSC's partnership with the States of Guernsey to deliver key national cyber security services pan-island is such an example, benefiting both islands. Further afield, the Pacific Islands have united behind such a regional agreement without relinquishing sovereignty: the Boe Declaration[21] includes cyber security as a strategic focus area and tackling cybercrime as a shared priority.

- **We will deliver against the Island's Strategy for Sustainable Economic Development and the Digital Economy Strategy to drive change in the dynamics, and spark growth of, the Island's digital economy.**
    - These strategies support growth to enable the development of a trusted and secure digital economy.

- **We will ensure 'Security by Design' is embedded in all digital services offered to Islanders, allowing trust and confidence in online services Government e-services lead by example**

- **We will ensure legislation and regulation are appropriate and proportionate to enable business growth and development, whilst still providing reassurance to Islanders about the safety and integrity of their digital interactions and data**

- **We will encourage a greater number of companies to offer cyber security technologies, products and services, and which meet independently verified or internationally recognised quality standards**

- **We will support and encourage the development of cyber related start-up companies. This will build upon**
    - Digital Jersey's accelerator programmes to recognise the importance growth opportunities of such companies
    - Initiatives funded by Impact Jersey to consider security and digital advancement as key enablers for growth
    - Research opportunities for small- and large-scale Jersey businesses to be capitalised on, where partnering with universities to help drive business innovation and growth and enable access to relevant leading-edge skills and capabilities

Jersey is uniquely placed to thrive on a trusted and cyber resilient digital ecosystem. One that we have all played our part in to build and keep secure.

[21] Boe Declaration on Regional Security | Pacific Islands Forum Secretariat

Delivery

Delivery is necessary to achieve our ambitions in this cyber security policy framework. An Action Plan will be released that outlines the short-, medium-, and long-term initiatives needed to achieve our policy ambitions. Working with key stakeholders and delivery partners, the proposed Action Plan will define clear accountabilities and responsibilities.

To ensure we remain on track, a delivery review board will be established with members representing the key delivery partners and stakeholders. Meeting quarterly, the delivery board will be responsible for driving delivery against the agreed Action Plan. An annual progress report will be published to highlight what has been achieved and raise awareness of delivery challenges. A commitment to delivery needs to be upheld, if the ambitions of this cyber security policy framework are to be met.

Measuring Impact

Assessment of Jersey's cyber security capabilities will help identify areas of strength and opportunities for continual improvement. Within the policy framework, the commitment to deliver against each of the five strategic priorities can be mapped against the Oxford Global Cyber Security Capacity Centre's '*Cybersecurity Capacity Maturity Model for Nations'* (CMM)[22]. This maturity model provides a structured approach to help jurisdictions enhance their cyber security resilience versus appropriate ambition.

The Cybersecurity Capacity Maturity Model evaluates the breadth of national capacity and capability a jurisdiction should demonstrate to effectively deliver cyber security and build cyber resilience. Assessment against the model can be made by the jurisdiction or through independent assessment by a team of researchers from Oxford. The data gathered provides an evidence-based report that benchmarks cyber security maturity, highlights gaps, and can be used to identify future capacity-building. Such assessments will feed into the delivery of future action plans, enabling the delivery board to demonstrate measurable impact against the vision - ***optimising Jersey's cyber security and cyber resilience, enabling Islanders and businesses to prosper.***

[22] https://gcscc.ox.ac.uk/the-cmm, published 2021

Consultation Questions

The Cyber Security Policy Framework consultation is open for 6 weeks, closing 2 September 2025.

You can submit your response:

- Online by completing the questions within this Microsoft Form: https://forms.office.com/e/hHNp8LmMLJ
- By email to economy@gov.je with the subject heading ***Cyber Policy Framework Consultation***
- By post to: FAO Digital Economy Team, Department for the Economy, Government of Jersey, Union Street, St Helier, JE2 3DN

The information you provide will be processed in compliance with the Data Protection (Jersey) Law 2018. Find more information in the Department for the Economy privacy notice.

The Government of Jersey may quote or publish responses to this consultation but will not publish the name and addresses of individuals without consent.

Types of publishing may include:

- sending to other interested parties on request
- sending to the Scrutiny Office
- quoting in a published report
- reporting in the media
- publishing on the Government website
- listing on a consultation summary

Confidential responses will still be included in any summary of statistical information received and views expressed.

Under the Freedom of Information (Jersey) Law 2011, information submitted to this consultation may be released if a Freedom of Information request requires it, but no personal data may be released.

Respondent Profile Questions

1. What is your primary role or affiliation?

(*Select one that best describes you.*)

☐ Individual/Island resident
☐ Small business owner or employee
☐ Large business or corporate representative
☐ Public sector employee
☐ Educator or academic
☐ Student
☐ Cyber security professional
☐ Non-profit or community organisation

☐ Other (please specify): _____

2. What sector do you primarily work in (if applicable)?

(*Optional – select one*)

☐ Financial services
☐ Technology or digital services
☐ Education
☐ Healthcare
☐ Government/public administration
☐ Retail or hospitality
☐ Legal or professional services
☐ Not currently employed
☐ Other (please specify): _____

3. How would you describe your level of cyber security knowledge?

(*Select one*)

☐ Expert – I work in cyber security or a related field
☐ Intermediate – I have some training or responsibility for cyber security
☐ Basic – I understand the risks and take basic precautions
☐ Limited – I rely on others for cyber security
☐ Not sure

- **4. What is your age group?**

☐ Under 18
☐ 18–24
☐ 25–34
☐ 35–44
☐ 45–54
☐ 55–64
☐ 65+
☐ Prefer not to say

5. Do you live or work in Jersey?

(*Optional – select one*)

☐ Yes – I live in Jersey
☐ Yes – I work in Jersey
☐ Yes – I live and work in Jersey
☐ No – I am responding from outside Jersey

Survey questions relating to the Cyber Security Policy Framework

1. How confident are you in Jersey's ability to protect its digital infrastructure and respond to cyber threats?
(Scale Options – select one):

☐ Very confident
☐ Somewhat confident
☐ Neutral
☐ Somewhat unconfident
☐ Not confident at all

2. If you are unconfident, what is the reason?
[Open ended question, *response limited to 500 characters*]:

3. Do you agree with the five strategic priorities in the cyber security framework?
(Options – select one):

☐ Yes
☐ No
☐ Unsure

4. If no, what do you regard is missing?
[Open ended question, *response limited to 500 characters*]:

5. Please rank the five strategic priorities within the cyber policy framework in order of importance to you (1 = most important, 5 = least important)?

(*Please rank in order of importance*):

☐ Strengthening cyber security within businesses, organisations, and for Islanders: *Ensuring everyone understands cyber threats, adopts protective measures, and can recover from attacks.*

☐ Continual development of an Island-wide resilient digital ecosystem: *Building strong partnerships, legislation, and infrastructure to support long-term cyber resilience.*

☐ Growing cyber security skills and capabilities: *Developing a skilled workforce and career pathways to support the Island's cyber future.*

☐ Responding to the rise in cybercrime: E*nhancing law enforcement capabilities and public awareness to combat digital crime.*

☐ Building a thriving cyber industry: *Fostering innovation, investment, and economic growth in the local cyber sector.*

6. What support or resources would help you or your organisation improve your cyber security practices?

Suggested Options (*Please tick all that apply or suggest others*):

[ ] Access to free or subsidised cyber security training
[ ] Clear, industry-specific cyber security guidance
[ ] Access to appropriate cyber risk assessment tools (e.g. Jersey Cyber Shield)
[ ] Access to expert advice from the Jersey Cyber Security Centre (JCSC)
[ ] Templates for incident response and recovery plans
[ ] Receive regular threat intelligence updates
[ ] Access to cyber security awareness campaigns for staff
[ ] Financial support or grants for cyber security improvements
[ ] Guidance on supply chain cyber risk management
[ ] Information on appropriate minimum cyber security standards
[ ] Cyber security peer networking or mentoring opportunities
[ ] Recommended cyber security online training
[ ] Proactive malware deletion by a trusted source
[ ] Other (please specify, *max 300 characters*): _

7. How do you think Jersey can better support the development of cyber skills and careers, especially among young people and underrepresented groups?

[Open ended question, *response limited to 1000 characters*]:

8. What roles should the private sector, educational institutions, and international partners play in strengthening Jersey's cyber resilience?

Suggested Options (*Please select those you believe are most important.*)

☐ Collaborate with Jersey Cyber Security Centre to share cyber threat intelligence
☐ Provide cyber security training and awareness for employees and customers
☐ Invest in secure-by-design technologies and services
☐ Participate in national cyber incident response exercises
☐ Support cyber skills development through internships, apprenticeships, and mentoring
☐ Embed cyber security standards in procurement and supply chains
☐ Partner with schools and universities to promote cyber careers
☐ Contribute to public-private cyber security forums or working groups
☐ Adopt and promote international cyber security standards and certifications
☐ Share lessons learned from cyber incidents to improve collective resilience
☐ Co-fund or sponsor cyber innovation and research initiatives
☐ Help raise awareness of cyber risks in underserved or vulnerable communities
☐ Adopt zero trust methodologies
☐ Other (please specify, *max 300 characters*): _____

9. What concerns do you have about the balance between cyber security, privacy, and digital innovation in Jersey?

Suggested Concerns (*Please select the top 3 concerns that matter most to you.*):

[ ] Overreach of government surveillance or data collection
[ ] Lack of transparency in how personal data is used or protected
[ ] Cyber security regulations stifling innovation or small business growth
[ ] Insufficient protection for vulnerable groups (e.g. children, elderly)
[ ] Inconsistent enforcement of data protection and cyber laws
[ ] Limited public input into digital policy decisions
[ ] Risk of digital exclusion for those without access or skills
[ ] Unclear accountability when data breaches occur
[ ] Over-reliance on private sector for cyber security solutions
[ ] Insufficient safeguards against misuse of AI and emerging tech Insufficient safeguards against misuse of AI and emerging tech
[ ] Other (please specify): _

10. Do you have any other comments or suggestions in relation to building Jersey's cyber security resilience that would support policy development?

[*Open ended question, response limited to 1000 characters*]: