

Cyber Security Policy Framework 2025-2040

Raising Jersey's Cyber Resilience

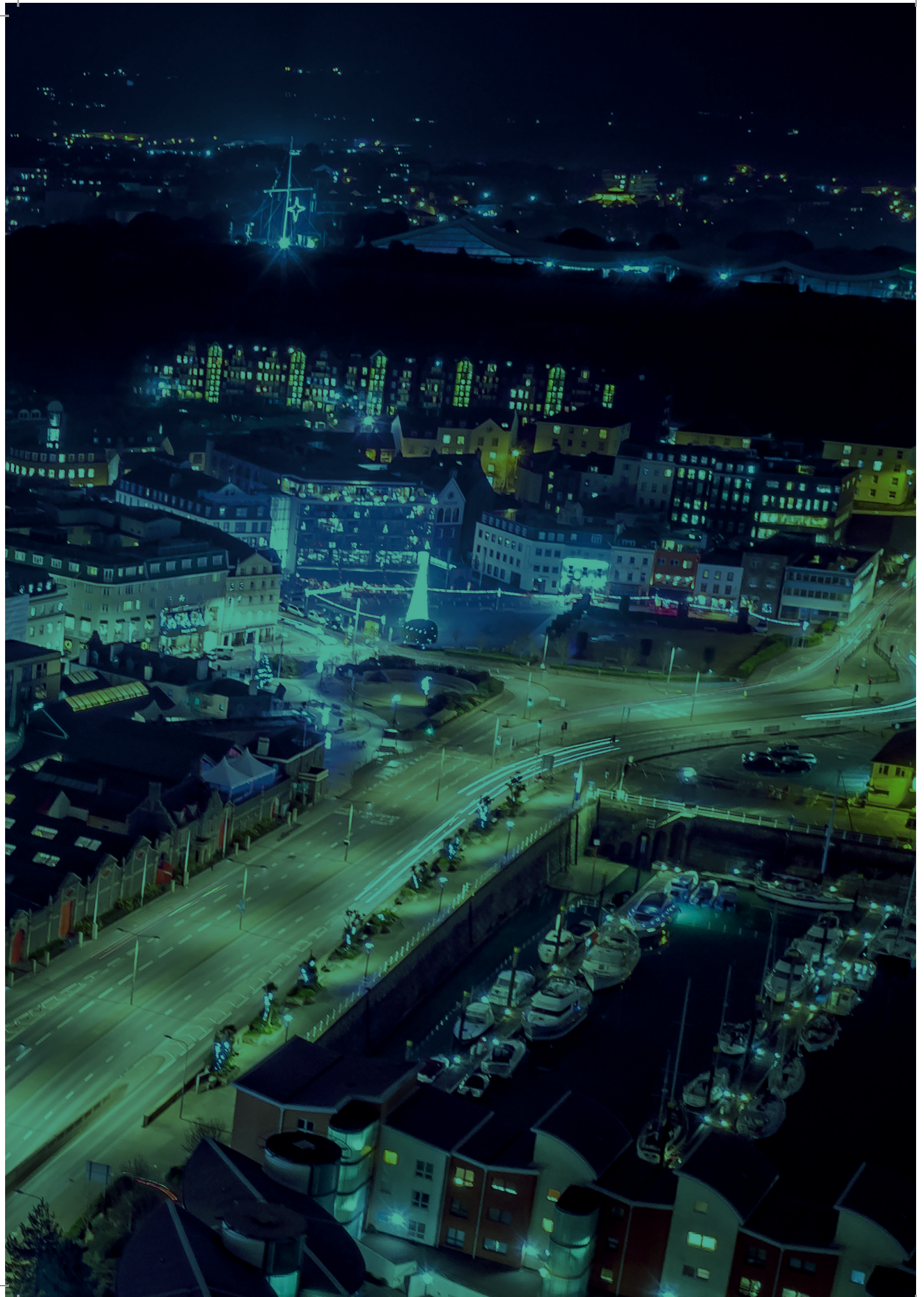
R.168/2025

NOVEMBER 2025



Contents

Ministerial Foreword	5
Introduction	6
Vision and Goals	8
Our Strategic Priorities	10
Strategic Partnerships	12
Strategic priority 1: Strengthening cyber security within businesses, organisations and for Islanders	14
Background	14
Policy ambition	14
Challenges	15
Implementation	16
Strategic priority 2: Continual development of an Island-wide resilient digital ecosystem	18
Background	18
Policy ambition	19
Challenges	20
Implementation	20
Strategic priority 3: Growing cybersecurity skills and capabilities	22
Background	22
Policy ambition	22
Challenges	22
Implementation	23
Strategic priority 4: Responding to the rise in cybercrime	24
Background	24
Policy ambition	24
Challenges	25
Implementation	26
Strategic priority 5: Building a thriving cyber industry	27
Policy ambition	27
Challenges	27
Implementation	28
Delivery	30
Measuring Impact	30



Ministerial Foreword



A secure and forward-looking digital environment is necessary for our Island community to thrive. Jersey's resilience, economic sustainability, democratic integrity and international reputation all are dependent on the quality of the Island's cyber security and cyber resilience.

Yet the internet has become a virtual minefield and war zone. Rapid technological advances are increasing the complexity of online risks, requiring a sophisticated strategic response.

This Cyber Policy Framework sets out the developmental direction of this important area of government policy and activity. As a small jurisdiction, we have less to invest in cyber security than many other jurisdictions and successful technology companies, but it cannot be treated as a sideshow. This Framework identifies the unique challenges faced by Jersey to meet its policy ambitions; and the cultural change that needs to be led by Government in which all Islanders will need to take part.

Obstacles include a lack of public awareness, a lack of funding and investment, and a lack of joined-up thinking. Cyber security is more than technology, however. It is about people, processes, partnerships and good practices, all working together to ensure our digital systems support the public good and protect our freedoms. It also offers the Island an opportunity for future economic development in a key area of innovation and global economic growth.

Cybersecurity is about community – one of Jersey's key strengths. By working together, we can forge ahead.

Government officers have engaged widely in shaping this Framework, drawing on expertise to shape its ambitions to address immediate threats and lay the groundwork for long-term resilience and prosperity. I thank everyone who has participated in its production.

Further engagement will be sought to inform its Action Plan. Government remains committed to continue to listen, adapt, lead and evolve as challenges change and new opportunities arise.

I invite all stakeholders to engage and partner with government to deliver on the policy ambitions set out in this document, to achieve a secure and successful digital future for us all.

A handwritten signature in black ink, appearing to read 'Moz Scott'.

Deputy Moz Scott

Assistant Minister for Sustainable Economic Development

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. Support 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 2040¹ 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 Strategy², 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.

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. Reports suggest cybercrime is now a \$10 trillion industry, affecting businesses, organisations and individuals, with additional state sponsored activity justifying the description of the cyber landscape as a war zone.

On Jersey, in 2024 alone, Islanders lost over £2.5 million³ to digital scams. The World Economic Forum⁴ highlights supply chain vulnerabilities as the biggest barrier to 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.

In this environment, and with the rapid emergence of new technologies that provide unprecedented computing power, the promotion, support and practice of high ethical standards within the local and international community will remain integral to the advancement of cyber security.

¹ See: *Strategy for Sustainable Economic Development*

² See: <https://statesassembly.je/publications/assembly-reports/2017/r-124-2017>

Lack of cyber awareness and under investment in cyber security ultimately is a cost borne by society as a whole. An Island-wide culture change is needed to develop shared cyber security values, attitudes, behaviours and habits and to 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 as a business investment. 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 with developments and to anticipate future challenges and cyber threats. Government has an important role to play, including in 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's 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 vision⁵ for 2040 through its own vision and a holistic and collaborative approach.

Vision

The vision of the Cyber Security Policy Framework is:

To advance Jersey in cyber security and cyber resilience, enabling Islanders and businesses to prosper

As defined by the UK's National Cyber Security Centre (NCSC)⁶, cyber security is how individuals and organisations reduce the risk of cyber attack. Its core function is to protect the devices we all use and the services we access – both online and at work – from cyber threats that can result in theft and damage. It is also about protecting from cyber attacks or compromise the vast amounts of data we access. Cyber security is primarily defensive, using controls such as firewalls, antivirus software, intrusion detection systems, encryption and secure authentication, regular security audits, vulnerability patching and access restrictions and protocols.

Cyber resilience, as defined by the NCSC, is “*an organisation's ability to maintain the correct operation of its essential functions even in the presence of adverse cyber events.*”⁷ Its focus therefore is on maintenance of business or operational continuity and how to respond or recover when a cyber attack succeeds. Methodology includes disaster recovery and business continuity planning, regular backups and failover systems, incident response and crisis management, replacing redundant systems and adaptive risk management.

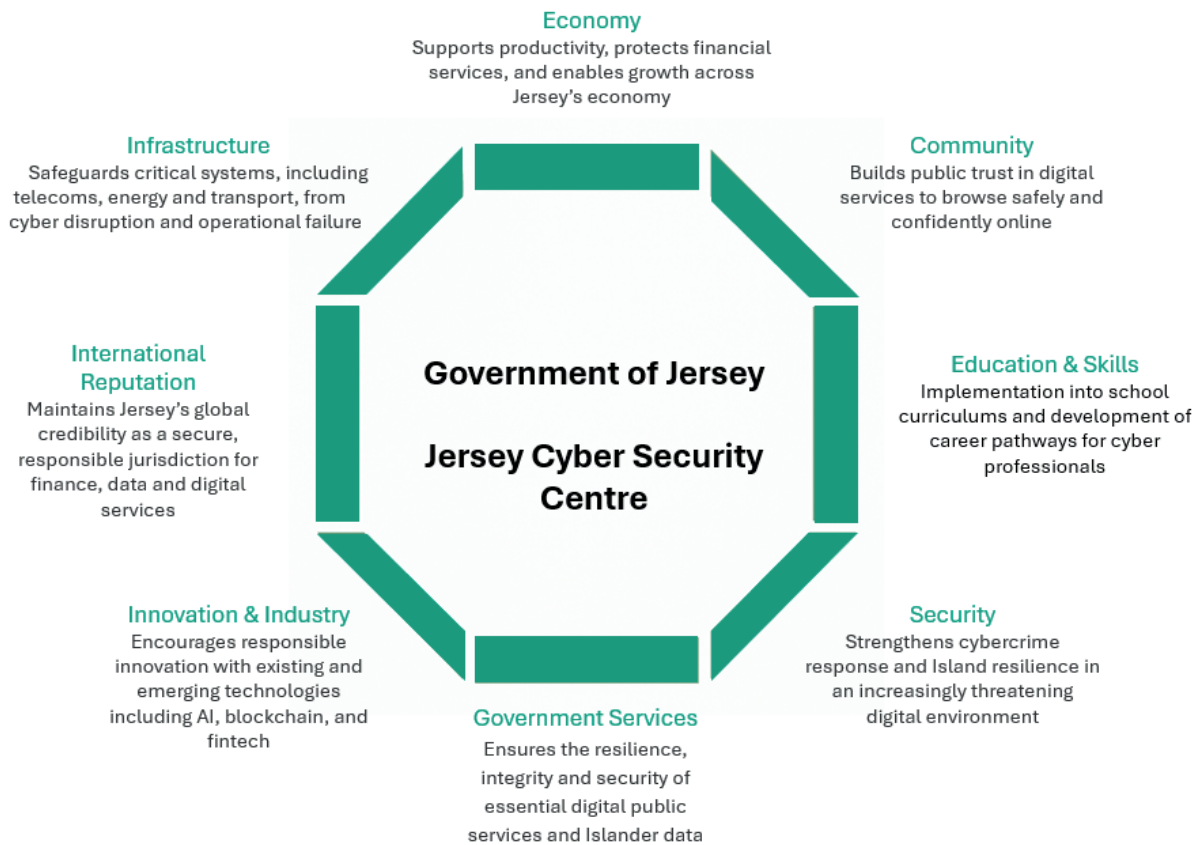
Overarching policy goals are:

- 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. The right level of investment in cyber security is hard to quantify.

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

⁶ See: [What is cyber security? - NCSC.GOV.UK](#)

⁷ See: [Introduction to the CAF Collection - NCSC.GOV.UK](#)



Commitment to deliver:

Choices:

To achieve delivery, prioritised choices need to be made. Based on the strategic ambitions in this framework an action plan will be developed to communicate and implement these priorities.

Concentration of Resources:

Budget and resource are both finite. Focusing delivery on key priorities will facilitate delivery.

Consistency:

The action plan will be constantly reviewed against the stated ambition, ensuring delivery of priorities that spans multiple years remains focused and does not succumb to scope creep.

Communication:

Vital for successful change, communication involves listening as well as making sure that everyone affected by the change is well informed.

Our Strategic Priorities

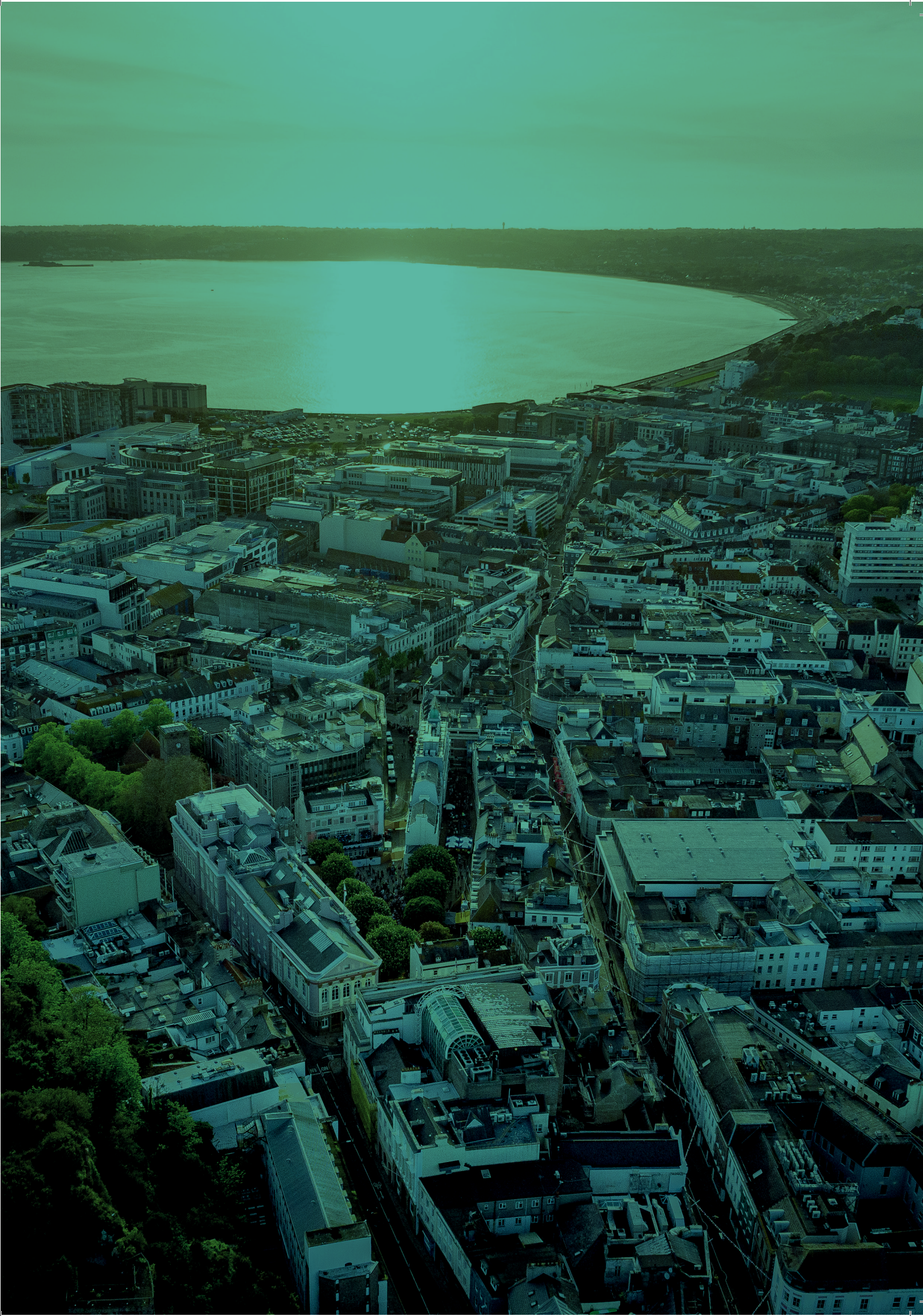
To achieve the vision of this Cyber Policy Framework, focused delivery will be measured against the following five strategic priorities:

1. **Strengthening cyber security and cyber resilience within businesses, organisations, and for Islanders:**
We will ensure businesses, organisations, and Islanders understand the cyber threats they face, supporting their adoption of 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 improve our knowledge, 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 enabled 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. These set out, for each strategic priority, the policy ambitions, priorities and current challenges Jersey needs to address, 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; and
- 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 reliant on resilient digital connectivity in our local businesses and for 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.

Work needs to continue across Ministerial portfolios and key strategic partnerships. These 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. JCSC is also uniquely positioned to enable Jersey to leverage technical expertise, extensive resources and sector expertise through building strong collaborative partnerships with larger or mature cyber security centres in other jurisdictions. Where appropriate, JCSC can then share relevant guidance and tools locally, avoiding the need to re-create.

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 targets of bad actors. 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 to continue to work in close collaboration with their key partners off-Island and to 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, advancing cyber security in the regulation of 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.

“ 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

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 their board rooms into their supply chains, providing necessary reassurance to clients and promoting shared cyber security attitudes, behaviours and habits. 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. Focus will be on collaboration, to avoid the need for Jersey to duplicate. These relationships must be preserved and fostered to achieve the aims of this framework.

STRATEGIC PRIORITY 1:

Strengthening cyber security and cyber resilience within businesses, organisations and for Islanders

We will ensure businesses, organisations, and Islanders understand the cyber threats they face, supporting their adoption of relevant protective measures and their recovery from a cyber attack.

Background

Throughout 2025, the crippling and devastating effects of cyber attacks on large and small entities routinely made global headlines. Some of these attacks could have been easily avoided.

Businesses and Islanders need to continually consider the risk-laden cyber environment in which they interact with on a daily basis. Businesses need to be able to reassure shareholders and customers that they are operating safely in a cyber environment in which the usual human ethical parameters often do not apply.

As defined by the UK's National Cyber Security Centre (NCSC), cyber security focuses on the *protection* of devices, services, network and the data stored on them from theft, damage or access by unauthorised access. Cyber resilience focuses on *the capacity* of an organisation to prepare for, protect against, detect, respond to or recover from a cyber incident. This is determined by the external threat capability of potential attackers.

Both cyber security and cyber resilience are foundational to enabling businesses and Islanders to confidently rely on, and take advantage of, current and future digital technologies.

Changing cyber threats need to be continually monitored and information on them shared. More importantly, appropriate action must be taken by businesses and critical and essential services.

More than 8,200 businesses are registered in Jersey, of which 89% have fewer than 10 full-time

employees.⁸ 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 may need help to engage competent professional assistance or to procure the best-suited services. A cyber incident can be costly and potentially devastating for them.

Navigating available cyber advice, and understanding the appropriate level of cyber security and resilience 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, resources and practices to be cyber secure and resilient by 2040.

Advice and guidance to be routinely sought and provided by JCSC.

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 and to include advanced counter measures to increasing AI threats. Key digital assets to be identified with tested contingency plans in

⁸ Jersey Business, 2023 Annual Report (p22) [jbl-annual-report-accounts-2023.pdf](#)

place 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 to be routinely sought and provided by JCSC.

This will enable Jersey to benefit from a strong digital economy where businesses, organisations and Islanders routinely use digital systems without fear, or recklessness towards risks, to boost their productivity, access services and support their daily lives.

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.

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 to be commonplace, reducing vulnerabilities and increasing resilience.

The JCSC to excel at providing threat information to essential services that is received and acted upon promptly. 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 businesses, helping them to reduce their vulnerabilities and deliver secure services. This will include 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 a mutually supportive and cyber security aware community to have been established Island-wide, where everyone understands the role they need to play to improve the Island's cyber resilience.

A culture where Islanders and businesses work together to continue to raise the cyber security of the Island and each knows how to get help quickly to reduce the impact of cyber attacks. This requires a culture change supported by a shift of attitudes, behaviours and habits Island wide.

From board members to business owners, charities to individuals, cyber will have progressed from a topic discussed purely within cyber professional networks to a widespread everyday appreciation of how to manage cyber 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.

Islanders and businesses to understand the security and resilience risks of utilising new technology (including AI applications) and know where to go to seek advice, help and support.

As technology changes, so should cyber security and resilience advice, in the form of guidance provided by JCSC and service providers, to ensure Islanders can confidently interact with Government and local businesses and other organisations utilising advanced technologies to provide services.

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

This is important to the building of both cyber security and cyber resilience.

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.

This is expanded upon in Strategic Priority 2.

Challenges

Cyber threats may feel 'invisible' and building cyber resilience may feel 'hard'.

Challenging this perspective will support our community. 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 by adopting appropriate cybersecurity measures and increasing awareness of threats. Rapid advancements in technology and the growth in online services and users require ever evolving solutions and continuous

updates of knowledge in which JCSC will have an important role to play.

To overcome a culture of associating the reporting of cyber incidents with regulatory requirements and a sense of 'failure' (rather than with good ethical practice and a shared learning opportunity).

Challenging this culture and perspective will encourage businesses to routinely and confidently share cyber incident information with JCSC and 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 in the wider community.

To drive a deeper appreciation of cyber security opportunities and risks in corporate strategic decision making.

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.⁹

Across the private sector and government, deepening cyber security and cyber resilience understanding at a corporate level could transform the delivery of trusted e-services for us all. A greater appreciation of the impacts or benefits 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. 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 of how to incorporate them safely 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 support 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 ways:

- 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 to raise capabilities and skills across all levels of organisations, irrespective of size.
- Joint awareness-raising efforts and collaboration across public-private initiatives to be realised and routinely assessed for effectiveness and support of 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 work towards an agreed baseline of cyber security related standards and good practices that are appropriate and proportionate to Jersey businesses, reflecting their size and their operational significance for the Island. Consideration will be given to balancing risk of exposure and likelihood of occurrence and severity (including societal and economic impact).

- Guidance to be available and accessible from JCSC to support businesses to achieve the relevant cyber security standards and good practice.

⁹ See *Boards Need a More Active Approach to Cybersecurity*, published May 2025

- A coordinated regulatory approach for cyber security to be established across Jersey's regulatory bodies to effectively monitor compliance.
- Jersey to focus on building collaborative partnerships with larger internationally recognised bodies, such as the NCSC, enabling their expertise, tools and guidance to be adopted locally, and only adapted where relevant.
- JCSC will have built good collaborative relationships with relevant partners both on- and off-Island to leverage their expertise for Jersey and enable timely sharing of information.
- Jersey businesses will have embedded good operational practices to ensure appropriate action is being taken, based on the vulnerability information received.

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 respond 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 also to be routinely shared with JCSC, raising resilience and reducing 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.

We will ensure threat intelligence and vulnerabilities are routinely collated by JCSC and shared with relevant Jersey organisations.

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:

- Protection of data to international standards, whether at rest or in transit, with sector specific guidance available.
- Deployment of up-to-date technological security controls and relevant security measures by both public and private sectors. These should reflect internationally established cyber security frameworks, standards and good practice, with sector specific guidance available.
- Routine testing of security measures and implementation of learnings.
- Security measures are routinely tested and learnings acted upon.

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

- For cyber risks to be routinely mapped, discussed and mitigated with appropriate and proportionate technical, operational and organisational measures being taken.
- 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. The right level of investment is hard to quantify

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.

STRATEGIC PRIORITY 2:

Continual development of an Island-wide resilient digital ecosystem

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

Background

This strategic priority considers our legislative, regulatory frameworks and the need to drive culture change within organisations, to ensure Jersey's digital ecosystem is sufficiently hardened to resist cyber attacks.

The digital ecosystem can be described as the interconnected network of digital technologies and human participants that co-create, exchange and interact online.

A resilient digital ecosystem can resist or recover quickly from attacks and continue to deliver essential digital services even under stress. This requires secure technology and networks, good governance, trusted supply chains, skilled people, and the flexibility to adapt to disruption.

Cybersecurity and cyber-resilience are central to a resilient digital ecosystem and are largely addressed by Strategic Priority 1. They must be reinforced by other critical elements such as:

- A robust infrastructure (reliable telecom networks, cloud platforms, and data centres with backup capacity, secure and resilient power and connectivity);
- Clear Legal and Regulatory Frameworks (data-protection, privacy, cybersecurity laws, standards for critical infrastructure and incident reporting);
- Effective Governance and Co-ordination (Island-wide strategies for digital resilience, public-private cooperation and rapid-response mechanisms);

- Secure Supply Chains (protection against vulnerabilities in hardware, software, and third-party vendors);
- Skilled Workforce and Public Awareness (cyber-literate professionals and informed users who reduce human-factor risks – addressed by Strategic Priorities 1 and 3); and
- Operational Continuity and Adaptability (Disaster recovery plans, regular testing, and capacity to evolve with emerging technologies and threats.)

Jersey's security legislative environment needs to continue to evolve. The recent Telecommunications Law (Jersey) Amendment Regulations and the 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: these could also 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 and trusted centre of excellence over time, to support digital ecosystem resilience.

The cyber risk profile of the digital estate of larger businesses, organisations and Government is much higher than other online users. Continuity of service is heavily reliant on the cyber security of their supply chain to avoid disruption to the delivery of critical and essential services relied on by businesses and Islanders.

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.

Prevention remains better than cure. Improving our cyber security can only be achieved by working together. The biggest weakness in any system often is people. We all need to take responsibility for completing relevant training and raising our own understanding of how we can protect ourselves and the organisations we work for and with.

Every business, individual and organisation has a plan in place to routinely test and improve the security of their systems.

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

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

Systems need to be routinely subjected to test their hardness to attack, and relevant encryption and cyber security standards deployed as standard, to ensure critical physical and digital infrastructure is protected.

For Jersey to have adapted and adopted international best practice into legislation and regulation to improve cyber security and resilience and minimise 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. Resistance to proportionate regulation can be managed with reference to learnings taken from the construction industry: the health and safety of the sector has significantly improved, with industry collaboration, through the adoption of appropriate legislative and regulatory frameworks.

For the Island's regulatory environment to be seamlessly aligned and to avoid red tape, duplication of the reporting of cyber incidents needs to be minimised while co-ordination in the sharing of information needs to be maximised. With emerging technologies providing innovation opportunities, regulatory thought leadership should provide reassurance that up to date cyber security standards are being 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 digital ecosystem resilience so that the Island can safeguard its international reputation, and economic standing, and have confidence in embracing emerging technologies.

For Islanders to understand the role of each Jersey based agency and where to turn to for relevant advice and support.

Agencies such as the JCSC, the Financial Intelligence Unit (FIU), Action Fraud, States of Jersey Police, and Jersey's regulatory bodies, need to develop closer collaborative working relationships to avoid duplication of effort and ensure clarity of their respective roles in a thriving ecosystem.

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

¹⁰ See: *Proposed Budget (Government Plan) 2025 - 2028 P.51-2024-(re-issue).pdf*

Challenges

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. The right level of investment in cyber security is hard to quantify but is vital for success.

Investment takes more than financial commitment. Improved cyber resilience will only be achieved by our whole community working together to heighten awareness of threats across all of the Island's Operators of Essential Services, share best practice, enhance cyber governance and hold each other to account.

The Government Budget has many pressures on it. Continued investment is needed to improve internal cyber security and resilience.

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

Each regulatory body in Jersey should consider the cyber security and cyber resilience of the entities they regulate to be critical regulatory considerations and should act as key partners in helping to raise cyber security standards and resilience. Closer collaboration will help provide thought leadership to proactively shape the future of Jersey's regulatory environment and how it should respond to fast-paced changes in access and utilisation of digital technologies.

Jersey is small but can capitalise on its international relationships, whether built through Government, regulatory bodies or centres of expertise. These relationships need to be maximised to drive change, as technology changes at pace. This will bring best practice, up-to-date thought leadership and technical expertise to the Island, ensuring safe use of innovative technologies and sharing threat intelligence. Such relationships are essential, where resource is constrained to develop this area firsthand.

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 or other organisation is responding to a cyber incident and needs to report to multiple bodies. Establishing clear cyber security standards will assist.

Clarity on recommended cyber security standards for non-regulated industries would establish a clear direction for cyber security resilience that the wider business community can unite behind.

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. We will work together with key strategic partners to avoid duplication and enhance the final policy outcome, so that it protects Islanders while supporting economic development.

Implementation

We will support Jersey-based centres of expertise and regulatory bodies helping to shape future digital policy, through:

- Continual review of the regulatory landscape to remove barriers and promote cyber incident 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 the need to balance digital security and privacy.
- Working to improve collaboration and to leverage local expertise to support Islanders and businesses as a whole.

We will work with board members and executives from all sectors, and especially Operators of Essential Services, to address cyber security risks through:

- Partnership with Jersey's Institute of Directors branch to deepen understanding and application of a risk-based approach to cyber security and governance at a corporate level;
- Ensuring corporate strategic direction and development is underpinned by robust cyber security risk management;
- Ensuring supply chain resilience is routinely reviewed and risk mitigation considered at a corporate level;
- Ensuring procurement processes consider relevant cyber security standards and best practices and routinely reflect: risk management, strategic physical infrastructure security, life cycle management, software and hardware assurance, outsourcing, and use of cloud services.
- Development and publication of procurement guidance for procurement standards and best practices by JCSC.

We will encourage supply chain resilience to be actively and routinely managed in all businesses, reducing the impact of disruption on the continuity of the service they provide to Islanders, with Operators of Essential Services leading by example, through:

- Identifying strategic assets and putting in place measures to protect them;
- Routinely testing the mechanisms put in place to protect strategic assets to ensure they are supported by contingency plans;
- Holding regular cyber resilience exercises that involve key supply chain partners, irrespective of whether they are based in Jersey or not. Learnings to be routinely shared for continuous improvement; and
- Regularly testing Jersey's emergency communication systems for cyber resilience.

We will leverage our international collaboration to highlight specialist cyber security capabilities that Jersey can rely on, including

- Building on the established collaborative partnership between the UK's National Cyber Security Centre, JCSC and Government; and

- JCSC representing Jersey's cyber security interests in key international fora and developing collaborative partnerships. Through these networks, JCSC will leverage cyber security thought leadership, bringing initiatives on island where impact can be measured.

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 and regulatory authority collaboration to:

- Continually review the impact of local legislative and regulatory frameworks and address gaps;
- Ensure the scope of the Island's Operators of Essential Services (OESs) remains relevant. Additional sectors that may be added include relevant health care, financial services and waste management services; and
- 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 identifies¹¹ digital and technology skills including AI, big data, computer networks and cyber security as critical for the future job market. There is need to build foundational awareness and an improved focus on developing advanced professional cyber skills.

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 show cyber security leadership at every level and a robust cyber security culture. Mandating training for all public sector employees and elected officials as a condition to access government operating systems.

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 update the Government's Digital Education Strategy¹² to address these inconsistencies and close these gaps.

Locally, the Channel Islands Information Security Forum¹³ (CIISF) has noted members find it difficult to attract and retain experienced cyber security professionals, with an acute gap within technical cyber security domains.

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

¹¹ See: [WEF_Future_of_Jobs_Report_2025.pdf](#), published Jan 2025

¹² See: [Digital Education Strategy report.pdf](#), published Oct 2022

¹³ See: [Channel Islands Information Security Forum \(CIISF\)](#)

¹⁴ See: [Schools - NCSC.GOV.UK](#) for Cyber First materials

training materials developed by the UK's National Cyber Security Centre (NCSC) CyberFirst¹⁴ 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 construction¹⁵, Jersey's digital sector, including cyber security, currently has no clearly identified 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 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 or identify an industry-led professional cyber security development body, or similar, to advocate for policy alignment, skills enhancement and industry-wide standards.

We will establish and encourage 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;

- Encourage local businesses to consider offering regular summer placements and internships for secondary and tertiary students;
- Structured work experience opportunities through programs such as Trident;
- Active corporate social responsibility programmes where local professionals engage directly with schools through adoption of programmes like CyberFirst; and
- A rolling programme of engaging public events, to raise awareness and excitement. Such events could include hackathons, competitions and more.

We will ensure comprehensive, ongoing training programmes 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 for all government and elected officials.

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

We will establish access to “cyber ranges” – a virtual environment that simulates real-world networks for cyber security training, testing and research.

- Providing a virtual battleground for testing the latest cyber security technologies and responding to real-world cyber threats, whilst enhancing the skills of our current and future cyber professionals.



¹⁵ See: [Jersey Construction Council \(JeCC\) - The Heart of Jersey's Construction Community](#)

¹⁶ See: [The UK Cyber Security Council Cyber Security Professional Standards Specialism Roadmap at Specialism Roadmap](#)

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 has developed strong international links to help fight cybercrime, a criminal activity that does not respect international boundaries. The States of Jersey Police's own Policing Plan states their strategic ambitions, supported by strengthening cyber resilience. Working alongside the Police, the Financial Intelligence Unit (FIU), the Economic Crime and Confiscation Unit, the Joint Financial Crime Unit, Jersey Fraud Prevention Forum and Jersey Cyber Security Centre all have a key role to play.

The impact of ransomware on local businesses and Islanders 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 and emerging AI technology reducing the barrier to entry for such criminal activities.

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. 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: those that do pay ransoms to release valuable data may not be aware that they could be inadvertently breaking Jersey's current sanction measures.

There is some evidence to suggest that a lack of prohibition on ransom payments in some jurisdictions is making those jurisdictions more vulnerable to ransomware attacks.

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. Collaborative information flows between all on- and off-Island law enforcement agencies is key to preventing cybercrime.

In collaboration with SoJP, the FIU and other relevant bodies, a clear policy on responses by businesses to ransomware attacks needs to be prioritised and communicated to the business community.

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 will be at hand.

Islanders to have the skills to protect themselves online, recognise non-legitimate internet sites and know how to validate information found online. A 'zero-trust' mindset to be prevalent amongst users of digital technology.

¹⁷ See: *Policing Plan 2025- 2028*

¹⁸ See: *2023-2030 Australian Cyber Security Strategy*

¹⁹ See: *Sanctions: Cyber-attacks — Jersey Financial Services Commission*

Businesses and organisations to take improved measures to keep personal data safe from attack, with systems routinely tested and vulnerabilities patched.

This will require the SoJP, Jersey Fraud Prevention Forum and Jersey Cyber Security Centre having a co-ordinated 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 fit for purpose to protect Islanders from emerging threats as technology rapidly advances and corresponding criminal activities develop.

Regular legislative reviews by multidisciplinary teams, to include the Island's financial crime agencies and regulatory bodies, to ensure Jersey's legal framework is fit for purpose as technology develops and use of emerging technology continues to challenge the status quo.

The interaction of legal frameworks between cyber security (technical aspects of security) and cybercrime (criminal justice response) to be properly considered, communicated and established.

Swift legislative updates to ensure criminal justice is served for cyber-related crimes.

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 appropriate resourcing, training and funding which currently is not at the level required.

The recent investment by SoJP of an extra £250,000 into their digital forensic unit currently is not 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 to prevent cybercrimes and speed up criminal proceedings to deliver timely justice for victims.

Jersey benefits from a very low general crime rate, creating a sense of complacency regarding security. Such complacency undermines readiness for protection from digital fraudulent activity that targets us in our homes, at work or on our mobile devices.

Unfortunately, many of these scams and frauds result in financial loss to Islanders. Scammers utilise AI to clone identities, including voices, making fraudulent activities harder to detect.

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, with practical tips and advice shared.

JCSC, FIU, Action Fraud and other local agencies need to increase cross-agency collaboration and support Islanders and businesses to take the necessary precautions and have the skills to identify fraudulent activity.

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

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

Jersey is starting its own cyber security legislative journey, with the proposed Cyber Security (Jersey) Law 202- aiming 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.

²⁰ See Recommendations 11 and 12 [VAWG Taskforce Summary Report.pdf](#)

The Violence Against Women and Girls Taskforce Report²⁰ 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 these nevertheless 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 businesses and Islanders:

- Embedding the roles and responsibilities of the different agencies on Island whilst promoting an inter-agency culture of collaboration;
- Co-ordinating awareness-raising campaigns to promote understanding of the scale, scope and impact of cyber related crimes for both businesses and Islanders;
- Supporting campaigns providing targeted materials for all business sectors and Islanders, to start building a culture of healthy scepticism when confronted with cyber related materials; and
- Raising awareness of ongoing developments in cybercrime: this reduces the impact of such crimes on businesses and 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; and
- Enable Jersey's Regulatory bodies to apply suitable enforcement powers to ensure cyber security standards are met and ensure Islanders are afforded relevant protection and feel safe in their interactions with advanced technologies (e.g. AI, quantum and other).

We will deepen a collaborative approach through:

- Leveraging international cooperation, leading to better information-sharing across borders and agencies, and access to relevant technical expertise e.g. enhanced digital forensic capabilities;
- Shared information between all on-Island agencies with law enforcement agencies, to avoid duplication and provide exceptional protection for Islanders (JCSC can play a key role in this network);
- Shared information between on-Island policy development, law enforcement and regulation bodies to highlight and address legislative gaps, regulatory challenges and policy hurdles; and
- Working with new and established partners to raise the profile of Jersey and enable Jersey to proactively adapt in challenging technology environments.

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

- Updated legislation with respect to payment of ransoms is due in Australia and the UK, with the impacts and benefits to be monitored as Jersey looks to protect businesses and Islanders.
- Education and awareness about the benefits and limitations of cyber insurance will be made available, allowing businesses to make an informed decision on how to protect their businesses.

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

Inward and local 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 investment.

The building of a successful cyber industry on the principle of 'secure by design' will be encouraged to ensure that security is embedded into products from inception. This proactive approach will minimise vulnerabilities, and support a more resilient digital infrastructure with reduced risks of cyber incidents. Security will be prioritised in software development, 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 and key industry player 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. Strong commitment and funding to modernise infrastructure needs to continue to support the technological advancements to support a robust cyber industry and growing digital economy

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 Jersey²¹ 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. Affordable living in the Island also is a key factor in keeping talent on-Island. While tech/cyber jobs pay salaries that are higher than in other sectors of the economy, access to affordable housing is important for workers in this sector too, particularly in less senior roles, and might be justified in terms of a higher level of economic contribution or essential public service provision.

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. Fostering a business-friendly environment will be a crucial first step for attracting investment and supporting local businesses and driving digital economic growth. The development of a fintech hub could create opportunities in this area.

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 to explore alternative approaches to policy development through recognised collaboration with other 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 and the network of Crown Dependencies to achieve more in less time 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 Declaration²³ includes cyber security as a strategic focus area and tackling cybercrime as a shared priority.
- Other international support mechanisms will be explored for these purposes such as the Forum of Small States.

We will deliver against the Island's Strategy for Sustainable Economic Development and the Digital Economy Framework.

- 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, providing trust and confidence in online services and reassurance and integrity of products and services.

We will encourage a greater number of companies to offer cyber security technologies, products and services that 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:

²¹ See: <https://impact.je/>

²² See: *The Challenges and Opportunities: How Jersey Can Become a Technologically Advanced Economy – Adapt Consulting Company*, published 18 October 2024

²³ See: *Boe Declaration on Regional Security | Pacific Islands Forum Secretariat*

- Digital Jersey's accelerator programmes to recognise the importance of such companies to economic growth opportunities;
- Exploring how initiatives can be funded by Impact Jersey in considering security and digital advancement as key enablers for growth;
- The capitalisation of research opportunities for small- and large-scale Jersey businesses, partnering with universities to help drive business innovation and growth and enable access to relevant leading-edge skills and capabilities; and

- Government Inward Investment and employee licensing initiatives.

We will improve the policy stance and guidance from Government and regulatory bodies to support the secure adoption of new technologies e.g FinTech, AI, quantum computing.

Jersey is uniquely placed to thrive on a trusted and cyber resilient digital ecosystem. One in which we must all play a part in to build and keep secure.



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)²⁴. 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 - ***To advance Jersey in cyber security and cyber resilience, enabling Islanders and businesses to prosper.***

Whilst the economic impact of strategic priority 5 (building a thriving cyber industry) may be hard to measure directly, case studies can serve as a recognised impact assessment tool and be used to measure the direct and indirect effects of this priority. They also can be used to explore a topic in depth and over time, providing lessons learned as well as measuring effectiveness or impact. Development of relevant case studies will be identified and will depend on the priorities identified in Action Plan.

²⁴ See: <https://gcsc.ox.ac.uk/the-cmm>, published 2021

