Information Security & Business Continuity Manager

Department: Justice & Home Affairs

Section: States of Jersey Police

Reports to: Head of Business Support & Shared Services

JE Ref: JHA060

Grade: CS12 **JE Date:** 28/10/2020

Job purpose

To lead at Senior Management Board on Information Security and Business Continuity providing strategic advice to the Chief Officer and other senior team members.

To design and lead the States of Jersey Police (SoJP) on the implementation of the Force Cyber / Information Security strategy and to ensure compliance with statutory, regulatory, and contractual requirements for Information Security of police information, data and assets.

To have management responsibility for the Data Protection Officer, ensuring that processes and disclosures are in accordance with the Data Protection (Jersey) Law.

Job specific outcomes

1. To review, develop, and monitor compliance of local Information Security Policies against national policy, court decisions and legislation.

2. To manage The data protection officer.

3. To chair the Business Continuity Group and have responsibility for the accuracy and testing of the Force's Business Continuity plans.

4. To undertake and perform a Force advisory role as a source of expertise and knowledge accessible to all members of the SoJP organisation for the areas of Information Security.

5. To reduce, and where possible negate, threats to the SoJP within areas relevant to Information Security and Force Compliance by appropriate action, inspection, and audit and policy development. To provide a suite of local operating procedures which are compliant to H.M. Government and national policing standards.

6. To conduct ongoing review and monitoring of SoJP Information Security measures in order to formulate detailed annual submissions in response to H.M. Govt. Information Assurance Maturity Model and the Security Policy Framework, and associated guidance on Codes of Connection for national policing systems. This activity is an essential requirement to ensure annual accreditation for continued connection and access to national information systems.

7. To report on security incidents and breaches, whether criminal or technical, and suitably identify risk to the reputation of the SoJP. To provide detailed reports and recommendations regarding such incidents and advise Force Senior Management of appropriate countermeasures to prevent similar issues arising.

8. To maintain expertise in the areas of Information Security and Force Compliance procedures by continuous professional self-development and training.

9. Provide the mechanism and support for appropriate training and education of staff in all matters connected to Information Security by provision of induction and other bespoke training as required.

10. To introduce and maintain a programme of proactive monitoring of police systems to identify misuse and/or activity which is non-compliant with Information Assurance standards and policy.

11. Cover any other ad hoc duties at the request of SoJP in pursuance of managing business support services requirements in a timely, efficient and effective manner.

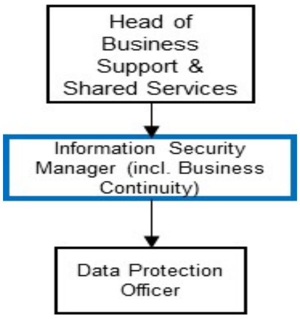
Statutory responsibilities

Active engagement, participation and compliance with any other statutory responsibilities applicable to the role, as amended from time to time.

This role is politically restricted. The job holder is not permitted to undertake political activity involving standing for election to the Government or as a Parish Constable, or publicly supporting someone who is standing for election or playing a public part in any political manner.

Organisation chart

Insert an organisation chart showing this role and its line managers and reports (individual names must *<u>not</u>* *be included only post titles)*


Head of Business Support & Shared Services
Information Security Manager (incl. Business Continuity)
Data Protection Officer

Person Specification

Specific to the role

Describe the knowledge, skills, experience, and qualifications required to perform the job to a satisfactory standard.

It is important to convey what the job requires, rather than what an individual might have, as these may be different. For example, you may have a postgraduate level qualification, however, an A' Level standard qualification is the requirement for the job.

ATTRIBUTES	ESSENTIAL	DESIRABLE
Qualifications *Please state the level of education and professional qualifications and / or specific occupational training required.*	Professional Qualification in Information / Cyber Security (e.g. CCP / CISM / CISA) and / or relevant experience; Qualification in Business Continuity Management (BCI).	Certification in Data Protection.
Knowledge *This relates to the level and breadth of practical knowledge* ***required*** *to do the job (e.g. the understanding of a defined system, practice, method or procedure).*	Knowledge or experience in understanding of Information Risk Management systems and processes; Knowledge of Data Protection law; Knowledge of operating across a number of systems and adjusting to specialist systems; Working knowledge of relevant systems (e.g. Microsoft Office), equipment, processes and procedures including standard software packages, with limited use of non-standard software.	People management skills with a strong understanding of how to communicate effectively

Technical / Work-based Skills
This relates to the skills specific to the job, e.g. language fluency, vehicle licence etc.
	Expert in Information Security for;
	Experience of Business Continuity plans;	

	Willingness to complete any necessary CDP in order to keep up-to-date with role specific requirements; Strong IT skills are essential, with the ability to interrogate systems storing sensitive and intelligence based data, analyse and interpret outputs and make informed decisions which may have far reaching consequences; Attention to detail and ability to record information accurately. Ability to manage, mentor and motivate any direct reports.	
General Skills/Attributes *This relates to more general characteristics required to do the job effectively, e.g. effective written communication skills, ability to delegate, motivation or commitment etc.*	Organised and self-motivated with the ability to work on own initiative, under pressure; Ability to accurately record information and data; Ability to plan and conduct reviews and monitor Information Security measures on behalf of SoJP in order to formulate detailed annual submissions; Be able to carry out established and continuing activities; Excellent numeracy, literacy and	

	communication skills essential.	
Experience *This is the proven record of experience and achievement in a field, profession or specialism.* *This could include a minimum period of experience in a defined area of work if required by an external body (for example a period of post-qualification experience).*	Practical relevant work experience in the provision of Information management security (including Data Protection) and business continuity; Evidence of working with confidential sensitive information, with the ability and experience to interpret procedures and law; Ability to identify and mitigate potential risks and develop and monitor compliance of local Information Security Policies against national policies, court decisions and legislation; Problem solving and influencing skills; Confident decision-maker; Accuracy and attention to detail, managing workloads and priorities; Experience in people management.	Knowledge or experience of Information Security in a Law Enforcement Environment
Criteria relating to Safeguarding *Other requirements needed to confirm suitability to work with vulnerable people e.g. attitudes, skills, experience etc.*	Exposure to unsavoury, confidential and sensitive issues where the careful and effective handling of such matters is essential. Requirement for high levels of integrity, tact, resilience and discretion, which are essential when dealing with sensitive intelligence and other information.	Emotional resilience.

Core Accountabilities, Attributes and Behaviour Indicators

Appointees to this role will be required to adhere to and perform their duties in line with the standards identified in the Government of Jersey Tier 4 core accountabilities attributes and behaviour indicators.

The standards relevant to this tier, identified in the Government of Jersey core accountabilities attributes and behaviour indicators, are to be attached in a separate document.