JOB DESCRIPTION

Job Title	Cyber Security Officer
Reports to	Cyber Security Manager
Reporting staff	None

Job Purpose

Supporting the Cyber Security Manager to provide direction and oversight of technical security requirements of ICT systems, providing expert risk and technical security advice and ensuring compliance with local and national security principles and standards.

Generic Responsibilities / Job Family

Specialist

To provide expert knowledge, advice and support to others within the Service OR to external parties regarding the Service and to ensure the provision of Specialist services in line with Service needs.

To establish, implement and maintain effective procedures and administrative systems including day-to-day financial administration and contributing to administrative planning for the function.

To represent the department/function at meetings and act as Service representative for initiatives as required.

To undertake project tasks or more specialised administrative work relating to the specific function or department.

To manage the collection, maintenance and integrity of data within Service systems and ensure the timely and accurate provision of information.

Specific Responsibilities	
1	Respond to cyber and information security incidents, including investigating and making recommendations to mitigate any risks.
2	Lead on the Service's implementation of Microsoft Purview and monitor and improve the Service's security posture across the M365 platform using Microsoft secure score.
3	Carry out internal audit checks of our Information Security Management System.
4	Work with Information Asset Owners and Leads to support the completion of impact and risk assessments for systems and information, to ensure that appropriate controls are in place and for both new systems and changes to systems.
5	Actively monitor and report cyber threat intelligence via National Fire Chief's Council's (NFCC) regional and national WARPs, the NCSC and other relevant security feeds.
6	Provide expert advice to ICT and managers on the appropriateness of security controls.
7	Embed a strong security culture through awareness training and improvement programmes, including updating the intranet and carrying out regular phishing campaigns.
8	Monitor activity logs for our ICT estate and investigate phishing reports and provide feedback to senders.
9	Represent the Service at local and national forums to enable best practice, information sharing, cyber threat analysis and collaborative working.
10	Assist the Cyber Security Manager in other work such as writing procedures, completing codes of connection, completing returns for standards, facilitating the annual IT health check.