Chief Security Officer

Reports to:	Head of Strategy and Technology		
Department:	Shared Technology Services	**Grade:**	Hay 5
DBS Status:	Basic	**Politically restricted:**	Yes

Job Purpose:

1. The Chief Security Officer serves as the process owner of all assurance activities related to the availability, integrity and confidentiality of partner Council information in compliance with the Councils' information security policies.
2. A key element of the CSO's role is working with executive management across all partner and customer organisations to determine acceptable levels of risk for the organisations.
3. This senior position is accountable for establishing and maintaining a Shared Technology Services' information security management program to ensure that information assets are adequately protected.

Values

Collaborate proactively.
Lead inclusively.
Embrace change.
Be bold and curious.
Celebrate and share our success.

Overall Description

The Chief Security Officer (CSO) is the senior lead responsible for safeguarding information assets across all STS partner councils. The role oversees the development and operation of the information security management programme, ensuring the confidentiality, integrity and availability of council data in line with organisational policies and regulatory standards.

Working closely with executive leaders across partner organisations, the CSO defines acceptable risk levels, leads cyber-security strategy, and ensures continuous improvement of security capabilities and resilience. The post manages multidisciplinary security teams and advises governance boards on risks, incidents and overall security posture.

Through strategic leadership, effective oversight and collaborative engagement, the CSO ensures that STS maintains secure, reliable and well-governed technology services for all partner councils.

The role involves managing a broad range of internal and external relationships, including directors, senior managers, elected members, and various public, private, and voluntary sector partners.

It requires developing strong partnerships, leading a high-performance team, and taking a key role in the development of council services.

The position operates within a framework set by the CEO and Council but allows considerable autonomy in shaping services. The role also leads on policy development, ensures compliance with new legislation, and upholds high professional standards.

The position is expected to be part of the Councils' emergency planning and resilience arrangement, including being on call Gold/Silver, and to demonstrate a commitment to embedding ownership throughout of this being everybody's business.

The postholder must conduct the duties in compliance with the Best Value Duty as set out in the Local Government Act 1999.

Job specific roles and responsibilities

1. Make a positive contribution to the delivery of the service, this will include working flexibly and positively to achieve the objectives of the council.
2. Manage and lead staff to achieve high performance and effective operational delivery, including developing and improving staff capability.
3. Manage a customer focused service and the effective use of resources.
4. Ensure that the council's overall vision, values and ethos are central to the requirements of the service.
5. Support effective working relationships and act as an ambassador and advocate with external organisations
6. Keep up to date with developments in service delivery and best practice to ensure the service performs effectively and to the highest standards.

7. Definition, scoping and creation of IT and Data Security strategies and Risk Management programmes enhancing the reliability and security of the IT systems, projects and underlying data at your organisation.
8. Develop and enhance an information security management framework
9. Develop the STS capability for identification and mitigation of cyber security threat across our entire IT environment and continuously improve our security posture.
10. Overseeing managers and teams that you are responsible for, allocating resources to ensure that staff deliver secure and robust IT solutions to any of the organisations identified and agreed requirements.
11. Overseeing planning and execution of necessary vulnerability audits, penetration testing or forensic IT audits and investigations. Ensure that outputs improve your organisations IT Security.
12. Liaise with executive level officers and other key stakeholders plus managers and IT Security risk-assessment staff under your remit.
13. Oversee the framework and governance to approve new IT solutions development with Shared Technology Services overall IT, Data and Information Security policies.
14. Oversee staff training in all the latest security awareness skills, check associated protocols, methodologies and procedures are implemented.
15. Ensure compliance with any related legislation, such as the Data Protection Act, ISO standards or relevant government regulations.
16. Plan budget allocations and associated financial forecasts relating to IT, Data and Information security.
17. Liaise with and manage your partners, stakeholders, vendors, and third party service or solutions providers.
18. Oversee projects, budgets and resources under your remit with a view to ensuring that Shared Technology Services gets a favourable return on it investments in staff, hardware, software and service providers.
19. Work directly with the partners and customer organisations to facilitate risk assessment and risk management processes.

20. Understand and interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services.
21. Provide leadership to the partners' information security organisation.
22. Partner with business stakeholders across Shared Technology Services to raise awareness of risk management concerns.
23. Manage the provision of information for Audits instigated by our partners and ensure that recommendations are tracked and enacted.
24. Make a positive contribution to the delivery of the service, this will include working flexibly and positively to achieve the objectives of the council.
25. Manage and lead staff to achieve high performance and effective operational delivery, including developing and improving staff capability.
26. Manage a customer focused service and the effective use of resources.
27. Ensure that the council's overall vision, values and ethos are central to the requirements of the service.
28. Support effective working relationships and act as an ambassador and advocate with external organisations
29. Keep up to date with developments in service delivery and best practice to ensure the service performs effectively and to the highest standards.
30. Safeguarding is everyone's responsibility and all employees are required to act in such a way that at all times safeguards the health and well-being of children and vulnerable adults.
31. Carry out duties with due regard to the Council's Customer Care, Equal Opportunities, Information Governance, Data Protection, Health and Safety and Emergency Planning & Awareness (including to provide assistance where available) policies and procedures.
32. Undertake any other duties commensurate with the general level of responsibility of this post.

Safeguarding is everyone's responsibility and all employees are required to act in such a way that at all times safeguards the health and well-being of children and vulnerable adults.

Undertake any other duties commensurate with the general level of responsibility of this post.

Essential Requirements (key skills & qualifications)
Knowledge and Qualifications

1. In-depth knowledge of information security principles, including confidentiality, integrity, availability, risk management frameworks, and cyber-security assurance, as required for establishing and maintaining an information security management programme.
2. Strong understanding of IT and data security strategies, including developing organisational IT security frameworks and risk-management programmes.
3. Knowledge of partner Council policies and governance requirements, including politically restricted responsibilities and compliance expectations across multi-authority environments.
4. Understanding of cyber-security regulatory standards and compliance frameworks, such as Cyber Essentials, CAF, and best-practice audit requirements.
5. Relevant professional qualifications in information security (e.g., CISSP, CISM, ISO27001 Lead Implementer/Auditor or equivalent).

Experience

1. Significant experience leading information security functions in a complex, multi-organisation or shared-services environment, including setting strategy and managing security programmes.
2. Experience working with executive leadership across partner councils or similar organisations to define acceptable risk levels and influence decision-making.
3. Experience managing cyber-security operations, including vulnerability management, penetration testing, forensic investigations, and security monitoring.
4. Experience managing multidisciplinary security teams, e.g., Cyber & Compliance, Security Monitoring, Audit & Compliance, Security Analysts.
5. Experience delivering IT security improvements and major programmes, including ZTNA, VPN replacement, SWG, device compliance, backup/recovery testing, and privileged access reduction.
6. Experience preparing and reporting to governance boards on cyber-security posture, risks, and mitigation activities.

Skills and Abilities

1. Ability to define, scope, and deliver organisation-wide IT & Data Security strategies, ensuring improved security posture across all STS environments.
2. Strong leadership and people-management skills, with the ability to allocate resources, manage managers, and ensure delivery of secure services across partner councils.
3. Excellent risk-management capability, including interpreting complex technical risks and translating them into executive-level recommendations.
4. Ability to oversee and improve security frameworks, ensuring compliance with partner council policies and national standards.
5. Strong analytical and problem-solving skills, particularly in vulnerability management, incident response, and audit findings remediation.
6. Ability to communicate complex security information clearly, engaging both technical teams and senior stakeholders across multiple boroughs.
7. Proactive and collaborative leadership style, consistent with STS values: collaborate proactively, lead inclusively, embrace change, be bold and curious, and celebrate success.

Budget Responsibility and Overall Headcount

Direct reports:

1x Cyber & Compliance Manager

1x Security Monitoring & Performance Officer

1x Audit and Complaince Officer

1x Security Analyst

Within reason these key deliverables may evolve to meet service need and it is expected that the postholder will be flexible and adaptable in their delivery to meet both service and council wide needs

Version: 1
Date of Job Evaluation: 04/03/2026