**A picture containing text

Description automatically generated**

**North Northamptonshire Council**

**JOB DESCRIPTION**

**DEPARTMENT:** Chief Executive

**POSTHOLDER SECTION:** Technology, Digital & Data

**GRADE: PS10**

**Job title:** Cyber Security Manager

Purpose of Job:

North Northamptonshire Council is going through a period of large-scale strategy and transformation to bring together our estates as well as create the world leading services for our citizens. We have an ambition to create brilliant and modernised services; to use modern platforms and infrastructure; and to make the best out of our investments in our technology and teams. This is a vital role in that journey, responsible for ensuring that we design and implement security right from the beginning of our journey, mitigating and managing technical risks to data and the organisation.

This role is responsible to the Chief Information Officer of North Northants Council for:

* provide expert advice on the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems.
* Provide leadership in defining and shaping our cyber security strategy, the design of our products and services, baking security into our standards and practice. This should be achieved alongside a expert balance in the management of information governance and controls to support the organisations ambition to be digitally flexible.
* Convey the value of security across the council, working with stakeholders at all levels to ensure that security is embedded and part of the organisation ethos.
* Ensure the organisation utilises legal, best practice and standards for security and leading on technical audits for the Council.
* Supporting our Digital approach and outcomes to impact residents and businesses through organisational strategy

Objectives and outcomes for this role;

Tasks linked to this role will include but not be limited to

* Direct responsibility for the leadership and development of enterprise-wide security architecture and processes which ensures that the strategic application of security is embedded in the organisation.
* Work closely with our DPO and information governance teams to shape our security stance on technology and information management.
* Working closely with Colleagues in West Northants and partners to deliver our Digital vision and roadmap effectively.
* Review our infrastructure and technology to analyse and assess their vulnerabilities, in order to build and execute plans to mitigate.
* Regularly monitoring and reviewing of our cyber stance, in order to update our strategy in line with our organisational ambitions.
* Engage with Senior and relevant stakeholders across the organisation to ensure that adequate measures are in place to support the integrity of the estate and data.
* Increasing Security awareness within the organisation and developing approaches to support these.
* Maintaining up-to-date knowledge of emerging security trends and developments in areas of interest to the organisation and utilising new approaches to develop our strategy and align.
* Analyse results of investigations into complex, or highly sensitive security violations or Breaches and determine any modifications to standards and their implementation.
* Review supply chain assessments, new business proposals and planned technical changes and provide specialist guidance on security issues and implications.
* Enabling the organisation in the compliance of areas such as GDPR, PCI, PSN and working towards standards such as ISO27001
* Developing and coaching the information security team and working closely with the Technology, digital and data management.
* Ensuring the organisation is focused with adequate levels of patching, firewall configuration reviews and SIEM alerting.
* Hold our partners/suppliers to account for spend, performance and behaviour, including diversity within their teams.
* Maintain and input for the risk register in the technology service, documenting details of any or all risks and their progress to remediation or mitigation.
* Manage staff performance appropriately by providing constructive feedback and take action where performance falls below the expected standard.

People management responsibilities;

This role will be;

* A management role in the Technology, Digital and Data service
* Responsible for the Security teams within North Northamptonshire
* Responsible for working alongside a team of staff

Work environment

* The post-holder will be required to deputise for the Chief Information Officer (CIO) from time to time.
* Participate/ work with external groups and stakeholders for the organisation such as NCSC, EMGWARP, auditors and accreditors as required.

**Person Specification**

|  |  |
| --- | --- |
| **Job Title** | Information Security Manager |
| **Grade** | PS10 |
| **Service/Section** | Technology, Digital and Data |
| **Directorate** | Transformation |

|  |
| --- |
| **Criteria** |
| **Technical Knowledge & Experience** |
| * Expert knowledge and understanding of security and system architectures; the relevant technologies, tools and platforms, best modern practice; industry trends and risks * A good working knowledge of information security including ISO/ IEC 27001 Information Security Management Standard and Cyber essentials. * A deep applied knowledge of agile ways of working * Experience of working across multiple channels (some or all of digital content, digital tools, assisted digital, webchat, phone, face to face) * Understanding of, and practical experience of applying GDPR, the Freedom of Information Act and other related legislation, standards and codes of practice * knowledge of infrastructure concepts, protocols and standards, including Active Directory, group policies, various hosting options, SSL, SAN, business continuity and disaster recovery. * High level of management, development and interpersonal skills. * Expert in understanding the business environment of the organisation and closely associated organisations and the organisation’s technical platforms. * Expert in understanding the functional structure of businesses and other organisations; their mission, objectives, strategies and critical success factors. * Experience with managing technology suppliers and partners * Certified Information Security Manager (CISM) or Certified Information Systems Security Professional (CISSP) certified * Experience of developing services that takes account of the needs of diverse users. |
| **Skills and Abilities** |
| * Ability to lead/ action the organisation’s cyber strategy and team. * Ability to lead during times of great change. * Ability to develop and get agreement to a strategy. * Ability to flex delivery approaches depending on context. * Passionate about building diverse teams and communities. * A strong influencer, with the ability to persuade and negotiate with stakeholders of all levels, including CEO, directors and elected members, including communicating methodologies and projects to a diverse, non-expert audience, and leading on the team’s remits, priorities and budget. * Strong people management skills, with the ability to create a positive working environment in which equality and diversity are embedded in every aspect of the team’s work and output, dignity at work is upheld and staff are empowered and motivated to achieve good outcomes. * Shows the ability to delegate effectively, empowering others. |
| **Equal Opportunities** |
| * Understanding of and commitment to the Council’s equal opportunities policies and ability to put into practice in the context of this post. * Understanding of and commitment to achieving the Council’s staff values and ability to put into practice in the context of this post. |