**JOB DESCRIPTION**

|  |  |
| --- | --- |
| **Job Title**  **Executive Director** | Chief Information Security Officer (CISO) – National Services Scotland (NSS)  No |
| **Location** | Flexible - Edinburgh or Glasgow |
| **Immediate Line Manager** | Director of Digital and Security |

|  |  |
| --- | --- |
| **2** | Job Purpose The primary purpose of this post is to provide National leadership at a strategic level across NSS, NHSScotland and the Scottish Government to develop and implement a strategy for the delivery of national Information Security and Governance services across NHS Scotland Health and Social care.  The Chief Information Security Officer (CISO) is responsible for leading the development and implementation of services that drives whole system behavioral change, facilitates Information and Cyber Security policies across health and social care and delivers significant value creation through the development of a shared service capability that can be replicated and implemented across the NHS in Scotland and other Public Sector organisations.  This post will provide senior leadership working at the most senior levels of Scottish Government, NHS Scotland and other Public Sector bodies with responsibility for leading and driving collaborative work to align Information and Cyber Security policy and administration with relevant regulatory, legal and ethical mandates.  The post holder will lead and drive the development and delivery of an enterprise service for Information and Cyber Security, Information Governance and Risk Management, by providing professional and expert leadership and building close and effective working relationships with key stakeholder and customers across the NHS and wider Public Sector. |
|  |  |

|  |  |
| --- | --- |
| **3** | **Dimensions**  The CISO is a core member of the Digital & Security senior management team who will lead a group of approximately 50 staff (comprising of professionals from Information Security, Information Governance, Cyber Security, Management and Support staff) who are geographically dispersed across a number of sites throughout Scotland, including the Cyber Centre of Excellence (CCoE) and the Security Operations Centre.  The postholder has prime responsibility for an operating budget of approximately £30m with additional funding from delivery of services to external parties that bring revenue generation. The postholder has a key role in directing further expenditure of an estimated £35m per annum.  The postholder will lead on optimising NSS and NHSScotland expenditure on Information and Cyber Security by developing and implementing an effective and efficient enterprise service using both permanent resources and expert 3rd party services to achieve a blended cost model with the required levels of expertise.  Both the number of staff directly employed and the overall budget will increase over the coming years as the strategy is implemented across a wide range of organisations as the demand for cyber security continues to grow due to the increasing threat posed in this domain. Therefore, the dimensions of this post may also increase and flex in size.  The CISO is a unique role in NHSScotland and has responsibility for innovation in Information Governance and Cyber Security which will require strong and effective leadership to question the status quo and lead people to be creative and collaborate across a wide range of organisations to ensure there are agreed standards, policies and solutions that are adopted at a national level through the CCoE . The post will require strong leadership, influencing and negotiating skills to work both within and beyond the NHS in Scotland to influence and inform the wider health and care system, by:   * + providing strong internal and external leadership in order for NSS to be the leading organisation to deliver Information and Cyber Security services across the NHS in Scotland   + enabling multi-disciplinary working across NSS, NHSScotland and Scottish Government through use of industry best practices for information and Cyber Security   + develop and maintain a strategic approach to Information Governance, Information Security and Cyber Security to support NSS locally and the wider NHS in Scotland, working with senior leaders to implement practices that meet agreed policies, frameworks and standards   + creates and owns a risk-based control framework that incorporates continuously changing environments that result from both national and global standards and regulations   + ensuring NSS complies with its legal duties relating to Information Governance, Information Security and Cyber Security * Collective responsibility for the achievement of the organisation’s strategic priorities and the delivery of agreed outcomes aligned to DaS commitments within NSS Annual Delivery Plan. * Maintaining focus at all times on delivering transformational change and demonstrating how the work of our teams is having an impact on the achievement of health and social care wider responsibilities. * Developing purposeful partnerships, which enable NSS to achieve its strategic objectives. In particular, continually determine that teams within each area of responsibility are efficient, effective and providing value for money. Ensuring delivery of core services while creating capacity for innovation and transformation. * Developing networks with colleagues in National and Local Government in order to ensure that each Director is aware of and can influence policy development which has a bearing on health outcomes. |

|  |  |
| --- | --- |
| **4** | **Organisational Chart** |

|  |  |
| --- | --- |
| **5** | **Role of Department**  The Digital and Security Directorate provides a complete range of Digital services including Infrastructure Hosting, IT Service Management, Clinical Informatics, Information Security & Governance, National Programme delivery, Digital Office and Data Services to a range of stakeholders including Health Boards, Scottish Government, Public Health Scotland and other public sector areas supporting health and social care delivery across Scotland.  The core purpose of the Information and Cyber Security function is to develop and deliver best in class solutions both within NSS and as a shared service nationally in a way that role models capabilities that can be replicated for other public sector bodies. This dedicated function has been created in recognition of the critical importance of Information and Cyber Security in the delivery of solutions to the health and social care sector in Scotland.  The Information Security and Governance pillar will provide effective strategies to ensure the rapid deployment of services and solutions across the national landscape. Exploring and driving implementation via a strategic roadmap of tools and techniques that enable NSS to be an effective partner to NHS Scotland in a way that helps maintain an established level of expertise.  Information Security and Governance leads on a range of local and national initiatives and services including:   * The Cyber Centre of Excellence that specialises in cultural awareness and strategy. This CCoE has been commissioned by the Scottish Government to lead and deliver to and on behalf of the NHS in Scotland * The Security Operations Centre that ensures the deployment of Information Security technologies, provides consultancy services and coordinates the implementation of services across NHS Scotland * Information Governance services across NSS, coordinating the implementation of Information Governance Frameworks and providing specialist advice locally and to both NHS Scotland and Scottish Government * The development of local and national policies, processes and initiatives that ensure the safety, privacy and recovery of information owned by the organisation, in line with regulations and legislation |

|  |  |
| --- | --- |
| **6** | Key Result Areas The Chief Information Security Officer will provide inspiring senior leadership to managers, staff, the Board and its Committees. The post will help to deliver a dynamic, effective and innovative approach to the strategy, planning, management and provision of a range of national, regional and local services to partners, including NHS Scotland, Integrated Joint Boards (IJBs), Scottish Government, Local Authorities, Community Planning Partnerships (CPPs) and the wider public and voluntary sector. This will require a significant contribution to the development of a clear, innovative and strong vision for NSS as a leader in Information Security and Governance services. The values, attitudes and behaviours demonstrated in this post will play a major part in influencing NSS’s culture and ethos, underpinning the success of the Board.  As part of the Digital and Security Senior Management Team, lead on the development of Information Security and Governance strategy, in order to ensure the organisation’s work adds maximum value to the collective effort across Scotland to improve health and wellbeing outcomes. Along with colleagues, the CISO will have responsibility for the delivery of the Information Security and Governance strategy and plan of the organisation and ensuring the teams / functions they directly manage recognise the requirement for multidisciplinary collaboration with other parts of NSS and wider partners. Ensure flexible use of resources to deliver products and solutions that support the delivery of the strategic plan.  Provide leadership and strategic direction through the development of an Information Security and Governance strategy that is focused on building a comprehensive approach to security programmes and in a way that demonstrates alignment with both NSS and NHS Scotland priorities. Ensure the provision of a range of core national services including the deployment of Information Security technologies, providing highly specialist and credible solutions and strategies that are specifically designed to deal with serious threats and incidents across the NHS in Scotland.  The post holder will be required to develop a longer-term (3-5 year) sustainable financial strategy in order to deliver and maintain the organisation’s Information Security and Governance strategy. This will require negotiating new models of external funding, development of a core budget to support the ongoing development of services and to continue to explore emerging technologies and trends within the Information Security and Governance industry.  Explore partnerships that will augment / complement services delivered by NSS that enables greater innovation and exploitation of available technologies. Work closely with national agencies, including NCSC, law enforcement agencies, the Cabinet Office, Scottish Government, NHS Scotland and other key stakeholders to fully understand the threat landscape and promote multi-agency responses.  As a member of the DaS Senior Management Team, with full responsibility for NSS Information Security and Governance strategy, help to ensure the highest standards of corporate and financial, clinical, staff and information governance and related compliance with all relevant legislation. Ensure that best use is made of assets entrusted by the Scottish Government. Ensure controls, systems and processes are in place, appropriate to a public body of the size and scale of NSS and to align with the legal duties relating to Information Governance, Information Security and Cyber Security.   1. Work with senior leaders, board members and other executives to establish acceptable levels of risk for the organisation, as well as making recommendations to key stakeholders about similar approaches. Develop methods to ensure consistent application of standards, frameworks and guidelines that can be replicated across the NHS in Scotland and ensures an approach that empowers stakeholders to own and accept levels of risk that are appropriate to them. 2. Define Information Security and Governance practices, lead the creation (and assure the ongoing relevance) of the strategy in collaboration with other executive officers. Institute an enterprise-wide operating model that is consistent with the capabilities and competencies required to execute the strategy. 3. Lead research, strategy creation and development of new Information Security and Governance services to expand markets, optimize value from services (directly and indirectly) and grow revenue and/or value. Expand the organisation’s research and innovation in all areas of Information Security and Governance, especially in emerging skills and technologies. The postholder must be knowledgeable in both internal and external business environments in order to ensure new products and services remain compliant with legislation and regulations in an ever-changing landscape. 4. Work closely with all areas of NSS Digital and Security on ensuring that Information Security and Governance is embedded into programme and project delivery processes through the provision of specialist advice and services. Create risk-based processes for the mitigation of information security risks throughout supply chains and provide oversight around the information collected, owned or controlled by or on behalf of the organisation and ensure that this is stored and processed in line with laws and other regulatory requirements. |
|  |  |

|  |  |
| --- | --- |
| **7** | **Assignment and Review Work**  Reporting to the Director of Digital and Security , the CISO has a high level of autonomy within NSS. The role will work across government policies and priorities at national and local levels, with a high level of independence of action associated with developing and implementing actions that improve health.  The post holder is fully accountable for leading and driving progress within the identified areas of responsibility and within the parameters of established national and local priorities, policies and procedures. A high degree of autonomous working and innovation will be required of the post holder which will in turn require the postholder to fully develop the capabilities of their teams.  Individual objectives will be agreed between the post holder and the Director and will be an outcome of the annual business planning cycle which will deliver the varied needs and requirements of the stakeholder groups noted earlier. These objectives will be monitored in accordance with the Performance Management Arrangements for Executive and Senior Managers.  The post holder will continuously review quality of work within own areas of responsibility and across the workstreams as to the relevance of content, challenging poor quality work where necessary. |

|  |  |
| --- | --- |
| **8** | Communications and Working Relationships The CISO will communicate with a wide range of senior staff across the organisation, the Scottish Government, NHS in Scotland, Local Authorities, national agencies and beyond; and with senior officials of external organisation’s across public sector bodies in Scotland. They will represent the organisation in links with Scottish Government. Several areas of operation are sensitive and high risk with a wide variety of regulators requiring effective engagement. Excellent communication skills are required in order to influence others and to direct the implementation of change. Strong presentation skills are required, as is the ability to express views and perspectives convincingly, coherently and compellingly using a variety of media.  NSS Information Security and Governance will operate beyond the boundaries of NHS Scotland, and beyond Scotland, to assist the broader public sector. The postholder must therefore engage with a broad range of senior level stakeholders, including Chief Executives, Local Government leaders, civil servants, politicians, professional representative bodies, senior clinicians and other significant public sector stakeholders, locally, nationally and internationally.  Excluding the postholder’s immediate line manager and their staff within NSS, the following are key working relationships, with examples of the purposes of these contacts:   * With the Executive and Non-executive Directors of the NSS Board to lead, shape, approve and implement the strategic direction, governance and performance of the organisation; also, to ensure the provision of information and support to the Non-executive Directors to enable them to effectively fulfill their roles as non-executives. * With representatives of the Scottish Government Health and Social Care Directorate (SGHSCD) to agree specific programmes, projects and other initatives. As required, to discuss and resolve difficult or controversial issues relating to national policy or problems of potentially high political or media interest. To respond to Parliamentary Questions and to help shape, take forward and support wider corporate management arrangements put in place by Scottish Ministers and COSLA Leaders. * With Chairs, Chief Executives, Directors and other Senior Officers of health and public sector organisations as a member of National Committees which determine national policy on health and care matters. * With Local Government Chief Executives and other senior members of Community Planning Partnerships (such as Police, Fire Service and third sector organisations) to identify and help improve health outcomes. * With Chief Information Security Officers (or equivalent) from other national public health organisations, academic institutions, and industry partners in other parts of the UK, in Europe and internationally to develop services and innovation in health care related environments. * With the marketing and communications team – e.g. to respond to media questions about relevant matters; * With national and local representatives of Trade Unions and Professional Organisations – e.g. for communication and/or consultation on major issues affecting staff, and to develop and maintain effective partnership working and staff governance. * Participate fully with Chief Executives, Chairs and senior colleagues across NHSScotland to co-ordinate, develop national initiatives and support within the remit of NSS in a manner that leads to the development of each organisation. |

|  |  |
| --- | --- |
| **9** | **Most Challenging Part of the Job**  To deliver a strategic agenda which is owned and led by a wide variety of stakeholders across health and social care.  To establish and maintain a new and dynamic corporate culture across the organisation that reflects the innovative, creative, influential and nationally focused nature of NSS as it engages and influences across health and care in Scotland.  Providing cohesive direction to a new, diverse, complex organisation, comprising staff groups from different organisational backgrounds and cultures, and ensuring effective stakeholder management across a very broad spectrum of interests.  Driving up adoption and usage of NSS Information Security and Governance services across NSS, NHSScotland and both National and Local government. |

|  |  |
| --- | --- |
| **10** | **Qualifications and/or Experience Specified for the Post by the Employing Authority**  The job requires an inspirational leader with significant demonstrable experience in the Information Security and Governance arena. Areas of specialism will include Cyber Security, Information Security, Risk Management, Information Governance and other IT related disciplines. They will require drive, understanding, vision, experience and political awareness necessary to provide clear and dynamic leadership in relation to advocating for and supporting local systems and influencing national policy makers.  **Qualification**   * Degree level in a relevant discipline with post-graduate qualification or equivalent experience would be desirable * Additional qualifications / memberships in relevant professional disciplines. * Evidence of continuing professional/personal development, including management and leadership development. * Certified Information Systems Security Professional (CISSP), Certified Information Security Manager, or certification in Risk and Information Systems control is desirable   **Experience**   * The postholder will have considerable experience of operating at a senior level in a diverse, complex, and expanding organisation, which requires the operation and understanding of matrix management skills. * In addition, experience of the NHS and the dynamics of the Healthcare system, or other complex organisation would be a distinct advantage. * Significant knowledge and experience of working with relevant legislator requirements, regulations and other frameworks associated with Information Governance, Information Security and/or Cyber Security * Demonstrable knowledge and experience of working with Information Security Management Frameworks such as ISO/IEC 27001, ITIL and COBIT * The postholder will require the highest levels of communication skills, and an open, supportive and visible management style in order to earn the confidence and respect necessary to deliver effectively the agenda on major change; to support the development of a culture that encourages initiative, individual and team responsibility and open communication that motivates staff.   **Competencies**   * **Leadership**: Communicates a compelling vision and provides visible and supportive direction and guidance that empowers, enables, motivates and develops staff to achieve NSS’s goals. * **Strategic Thinking**: The ability to transform strategy into implementation planning and project/change management to deliver significant and measurable outcomes. * **Improving Quality**: Focuses on continually improving outcomes for customers, patients and other stakeholders. * **Achieving Results**: Develops and implements SMART service plans and reviews own team and service performance against these. * **Political Sensitivity**: Fostering and building effective alliances underpinned by a strong ethos of partnership working with a broad range of stakeholders to enable effective working at a national level within Scottish Government, Local Government and across NHS Boards and partner organisations. * **Working in Partnership**: Builds effective relationships with staff, customers and other stakeholders. * **Improving Performance through Team-working**: Works effectively as a team member and leads their staff with tenacity to deliver shared goals. * **Caring for Staff**: Creates a healthy, safe and dynamic working environment with a staff wellbeing ifocus and individuals are supported and motivated effectively * **Communicating effectively**: Communicates clearly and consistently and ensures that staff, customers and other stakeholders are influenced and engaged fully in service planning and delivery. * **Promotes a Learning Organisation**; Views learning as integral to service planning and delivery and develops organisational learning plans to maximise staff potential.   **Demonstrates through behaviours and actions an absolute commitment to NSS Values** |