Job Description

Post title: Chief Information Security Officer (CISO)	**Post No:**
Organisation Unit: Digital Technologies	**Date compiled:** 8th May 2019
Grade: Support Head	**Hours per week:** 37 **Weeks per year:** 52

If fixed term, state duration:

Immediate line manager: Director of Digital Technologies

Designation and grade of any staff supervised by the postholder: None

Job purpose:

Reporting to the University's Director of Digital Technologies, the Chief Information Security Officer will lead and own the University's information security strategy, drive and be accountable for a comprehensive approach towards information security across all areas of the organisation. The post holder will advise the University at a strategic level on existing and emerging threats and establish and lead the IT security organisation within the University, managing the risk to the University's IT facilities and maintaining awareness of both internal and external threats.

Principal duties and responsibilities :

- Leads and owns the information security strategy for the University. Provides ongoing leadership to the organisation on matters relating to Cybersecurity;
- Ambassador for Cybersecurity across NTU, increasing awareness and taking accountability for information security and management amongst key user groups. Influences and drives positive behaviours around information security;
- Contributes to overall business technology planning, providing a current knowledge of and future vision for security technology and systems;
- Develops, implements and monitors a strategic, comprehensive enterprise information security and IT risk management programme. Drives and owns the approach to information security risk;
- Leads cross University information security activities, managing the information security risk to IT facilities from internal and external threats.
- Develops and enhances an information security management framework;
- Acts as a Partner to business stakeholders across NTU, raising awareness of risk management concerns; facilitating risk assessment and management processes.
- Understands and interacts with the wider Digital Technologies function to ensure the consistent application of policies and standards across all technology projects, systems and services;
- Maintains relationships with Heads of College, Schools and Professional Services departments to enable an understanding of the University's IT landscape;
- Works with key staff within Digital Technologies;
- Defines, scopes and executes Data Security strategies enhancing the reliability and security of the IT systems, projects and underlying data at NTU;
- Drives external supplier strategy management, ensuring alignment between security stance of NTU and that of the vendor base;
- Frequents and represents the University at national and international information security networks, seeking best practice examples and opportunities to share these;
- Establishes and maintains relationships with counterparts at comparable institutions to achieve an understanding of the common risks and best practice;
- Liaises with external regulatory and law enforcement agencies on IT security issues;

- Supports the internal auditors to assist them in producing an audit programme that matches the needs of the University;
- Owns, manages and develops appropriate information security policies, procedures, controls and the overall information security governance framework.

Special requirements:

****

All staff are expected to comply with the University's Health and Safety and Equal Opportunities policies in the performance of their duties.

N.B.   The postholder may be required to undertake any other duties which may reasonably be required as within the nature of the duties and responsibilities of the post as defined, subject to the proviso that normally any changes of a permanent nature shall be incorporated into the Job Description in specific terms.

Job description drawn up by	John Murphy	Date May 2019
Approved for department by	Steve Denton	Date May 2019

See also
JD Guidance Notes

Person Specification

Post Title: Chief Information Security Officer (CISO)		Post No:
Organisation Unit: Digital Technologies		

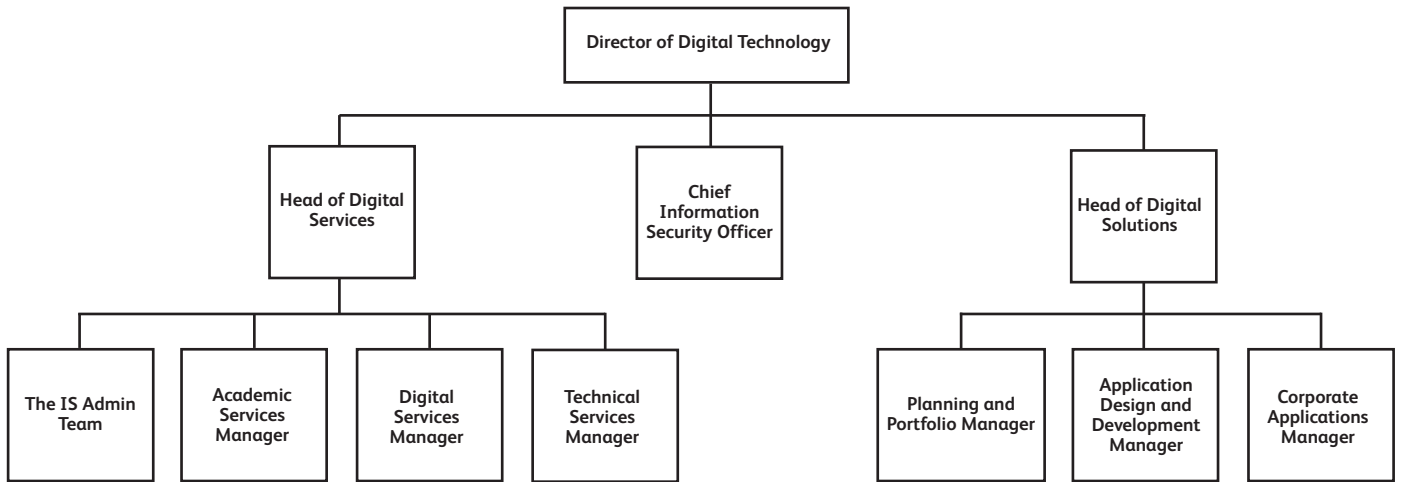| Attributes	Essential	Desirable
Knowledge	Up to date knowledge of key information security technologies; Knowledge of risk management techniques and best practice.	Knowledge and experience with key national and international information security and digital data standards, legislation and guidance relevant to the academic and research sectors Knowledge of data classification techniques.
Skills	Demonstrable high-level strategic thinking and planning skills; Demonstrated ability and experience in establishing, tracking, measuring and weighing information security risk; Demonstrated ability to operate within a secure environment on sensitive data, data request and information security incidents against strict information security policies. Demonstrated ability to build relationships at different levels of the organisation; Able to build personal and organisational brand externally, and to network with relevant organisations and individuals; Excellent presentation skills and the ability to create persuasive and accessible presentations to non-specialist staff at many levels of the organisation; A demonstrable commitment to leadership development of self and others as it relates to this area of professional specialist work;	An understanding of the PRINCE II and the factors that are critical to success of technical and business change. An understanding of IT service management and processes for service excellence.

Experience	Experience as an information security professional – especially in the area of information security strategy, with associated knowledge of governance, policy creation & maintenance, and monitoring and compliance A proven track record of creating and maintaining an information security service and developing, maintaining, implementing and embedding information security policy in a large institution or organisation. Specifically, proven experience in having dealt successfully with information security incidents. A proven track record working within a risk or information security governance structure. Experience advising, managing and protecting strictly confidential data and datasets or other classified data. Experience Implementing and/or maintaining formal best practice information security compliance or certification (e.g. ISO 27001/2, ISF the Standard of Good Practice for Information Security, COBIT) Experience of evaluating, creating, managing and providing information security training.	Experience building and maintaining a strong information security and risk governance structure within a large organisation. Experience of acting as chair of governance committees or boards.
Qualifications	Graduate calibre with degree or equivalent. Formal certification (CISSP, CISM or CRISC) and/or formal training in information security standards and best practice (e.g.: ISO 27001/2, ISF the Standard of Good Practice for	Current member of IISP (the Institute of Information Security Professionals)

	Information Security, COBIT)	
Competencies (where applicable)	Capable of working with and earning the respect of senior customer stakeholders. Able to articulate and agree a clear vision for the information security strategy.	

See also
[PS Guidance Notes](#)

Digital Technologies Organisation Chart
April 2019

```
                          ┌─────────────────────────┐
                          │ Director of Digital      │
                          │ Technology               │
                          └─────────────────────────┘
                                      │
        ┌─────────────────────────────┼─────────────────────────────┐
        │                             │                             │
┌───────────────┐           ┌───────────────┐             ┌───────────────┐
│ Head of       │           │ Chief         │             │ Head of       │
│ Digital       │           │ Information   │             │ Digital       │
│ Services      │           │ Security      │             │ Solutions     │
│               │           │ Officer       │             │               │
└───────────────┘           └───────────────┘             └───────────────┘
```

| The IS Admin Team | Academic Services Manager | Digital Services Manager | Technical Services Manager | | Planning and Portfolio Manager | Application Design and Development Manager | Corporate Applications Manager |

(NB: all roles have line management responsibility)

How to Apply

Nottingham Trent University has engaged the services of GatenbySanderson to whom applications should be sent by the closing date of 10 June 2019.

Chief Information Security Officer (CISO) - How to Apply

To find out more about the role and to apply, please visit: https://www.gatenbysanderson.com/job/GSe53296

For a confidential discussion, please contact our advising consultants at GatenbySanderson: **Stephanie Wilson on M: 07880 382745**, or **Phillippa Dunlop on 07807 631 564**, or **Adrian Barlow on M: 07393 011150**

Closing Date: 10 June 2019

To apply for this role, please submit an up to date copy of your CV, along with a Supporting Statement (no more than 3 pages) that addresses the criteria set out in the person specification, using examples to demonstrate how you meet the essential requirements. Please provide your home, work, mobile and email contact details and let us know of any dates when you are not available or where you may have difficulty with the indicative timetable. You should also provide the names, positions, organisations and contact details for two referees, one of whom should be your current or most recent employer. We will not approach your referees without your prior permission.

Once you have submitted your application, you will receive an automated email to confirm that you have applied. If you do not receive this email, please make contact with GatenbySanderson.