JOB DESCRIPTION

Department: IT Services
Job title: Head of Cybersecurity or AD – Cyber Security
Post Grade: Grade 9
Responsible to: IT Director

Position Summary

- Provides strategic leadership and guidelines on cybersecurity and information assurance, cybersecurity expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls.

- Develops strategies for ensuring both the physical and electronic security of automated systems.

- Ensures that the policy and standards for security are fit for purpose, current and are correctly implemented.

- Reviews new business proposals and provides specialist advice on security issues and implications.

- Obtains and acts on vulnerability information and conducts security risk assessments for business applications and computer installations; provides authoritative advice and guidance on security strategies to manage the identified risk.

- Investigates major breaches of security, and recommends appropriate control improvements. Interprets security policy and contributes to development of standards and guidelines that comply with this.

- Performs risk assessment, business impact analysis and accreditation for all major information systems within the organisation.

- Ensures proportionate response to vulnerability information, including appropriate use of forensics.

- Drafts and maintains the policy, standards, procedures and documentation for security.

- Monitors the application and compliance of security operations procedures and reviews information systems for actual or potential breaches in security.

- Ensures that all identified breaches in security are promptly and thoroughly investigated.

- Ensures that any system changes required to maintain security are implemented. Ensures that security records are accurate and complete.
Main Responsibilities and Tasks:

1. Develops cybersecurity policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.

2. Prepares and maintains a business strategy and plan for cybersecurity work which addresses the evolving business risk and information control requirements, and is consistent with relevant IT and business plans, budgets, strategies.

3. Operates as a focus for IT security expertise for the organisation, providing authoritative advice and guidance on the application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.

4. Manages the operation of appropriate security controls as a production service to customers.

5. Develops implementation approach, taking account of current best practice, legislation and regulation. Ensures implementation of cybersecurity strategy in automated systems and ensures operations of security systems. Analyses results of investigations into complex, or highly sensitive security violations, to determine whether standards are fit for purpose, are current and are correctly implemented.

6. Reports any significant breaches in security to senior management. Interviews offenders in conjunction with the relevant line manager or on own authority if the breach warrants it. Where appropriate, participates in forensic evidence gathering, disciplinary measures, and criminal investigations.

7. Ensures that procedures are in place for investigation of system access enquiries referred by support staff and for handling all enquiries relating to cybersecurity, contingency planning as they affect the activities of the organisation, function or department. Authorises implementation of procedures to satisfy new access requirements, or provide effective interfaces between customers and service providers.

8. Devises new or revised procedures relating to security control of all IT environments, systems, products or services in order to demonstrate continual improvement in control including creation of auditable records, user documentation and security awareness literature.

9. Authorises and initiates the provision of training, guidance and support to other security administrators and their agents within the employing organisation, in all aspects of security policy and control.

10. Reviews new business proposals and planned technical changes and provides specialist guidance on security issues and implications.

11. Maintains knowledge of the technical specialism at the highest level.

12. Keeps in close touch with and contributes to current developments in the technical specialism within employing organisation, own industry and in appropriate professional and trade bodies.

13. Is fluent at articulating best practice and is a recognised authority in the technical specialism.

14. Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, cybersecurity, purchasing etc) and advise colleagues and end-users accordingly.

15. Carrying out any other related duties as directed by the Assistant Director - Core Service Delivery.

Any other duties as required by the line manager or Head of Department that is commensurate with the grade.

As the needs of the College change so the above job profile, duties and location of the role within the Faculty of the College will be adjusted accordingly.
Skills and Competencies

Technical

1. Experience in delivering solutions using new and emerging technology/policy and industry best practice
   a. Managing resources (including external partners and staff) in order to deliver solutions in a managed timely process

2. In depth knowledge of cybersecurity landscape
   a. Policy
   b. IT Technology
   c. Legal
   d. Compliance
   e. Security testing
   f. Network, systems and application structures and best practice

3. Development methodologies and best practices
   a. Experience of various development approaches (e.g. waterfall, spiral, RUP, Agile)
   b. Experience with quality assurance procedures (e.g. testing, acceptance, source code control, configuration management, change management)
   c. Ability to design a security ecosystem from given requirements specification and document the design produced to agreed standards.

4. Application Support and Troubleshooting Knowledge
   a. Experience with using service desks (any package)
   b. Experience of ITIL or service desk practices
   c. Demonstrate a logical approach to service delivery

5. Ability to Write Documentation
   a. Ability to write for various audiences
   b. Ability to select appropriate document formats

Personal

- Planning, Organising and Personal Time Management
- Strong interpersonal, communication and presentation skills.
- Ability to convey detailed technical information to a variety of audiences including senior management.
- Proven analytical and problem solving skills.
- Positive personal qualities including business focus, drive, professionalism, integrity and teamwork.
- Willingness to identify fresh approaches and recommend where appropriate.
- Strong customer service focus.
- Appropriate attention to detail
- Networking particularly in application and development communities via various channels
- Experience and interest in technology roadmaps and innovation and an ability to identify opportunities to apply new technologies.
- Ability to transfer and augment existing knowledge and experience and an enthusiasm to learning new skills.
- A proactive approach to problem management and personal development.
- Ability to work in small teams, including matrix and virtual teams