



AHDB JOB DESCRIPTION	
Job Title	Information Security Manager
Department	Finance & Business Services
Location	Stoneleigh
Grade	Indicative salary £35-45k
Line Manager (Job Title)	IT Manager
<p>MAIN PURPOSE OF THE DEPARTMENT AND JOB</p> <p>The main purpose of the IT department is:</p> <ul style="list-style-type: none"> • The provision of Information and Communications Technology (ICT) expertise and the maintenance of ICT equipment, including software, hardware and peripherals in accordance with an agreed ICT strategy. • Provision of a network which gives AHDB the ability to collect, process and disseminate data on agricultural markets in order to promote efficient production and marketing of each sector of AHDB's activities. • To ensure a tested Disaster Recovery process is in place. • To ensure that system security is paramount. • To research and develop new projects to improve the effectiveness of AHDB's operations. <p>Under the supervision of the IT Manager:</p> <ul style="list-style-type: none"> • Responsible for the development and delivery of a comprehensive information security program across the organisation (to cover information in electronic, print and other formats). • Put in place processes and procedures to ensure that information created, acquired or maintained by AHDB (and its authorised users) is used in accordance with its intended purpose. • Responsible for the protection of AHDB information and infrastructure from external and internal threats. • Ensure that AHDB complies with statutory and regulatory requirements regarding information access, security and privacy. • Provide a source of expertise, advice and guidance on all information security matters to colleagues throughout AHDB. • Advise and guide AHDB toward ISO 27001 accreditation. 	
<p>DIMENSIONS: AUTHORITY LEVELS & DECISION MAKING</p> <p>To be Advised</p> <p>Budgetary responsibility:</p> <p>To be Advised</p>	

WORKING RELATIONSHIPS/MAIN CONTACTS/CONTEXT

Internal

IT Manager, IT department staff

Director of Finance & Business Services

Sector and Divisional Directors

External

IT Suppliers

IT Service Providers

KEY RESPONSIBILITIES

1. Work with the Senior Executive Team and IT Manager to develop information security policies, standards, procedures and guidance documentation; ensuring that they support compliance with statutory and regulatory requirements.
2. Over see the dissemination of policies, standards, procedures and guidance throughout the organisation.
3. Develop and deliver a program of education and training for all staff covering information security matters.
4. Assess organisational compliance with all statutory and regulatory requirements, working with Information Asset Owners to address any shortfalls.
5. Work with Information Asset Owners to ensure divisional Information Asset Registers are current and accurate.
6. Develop and implement an Incident Reporting and Response system to address security incidents (breaches), respond to alleged policy violations and handle enquiries or complaints from external parties.
7. Serve as the official AHDB contact for information security and privacy incidents, including relationships with law enforcement bodies as necessary.
8. Develop and implement an ongoing risk assessment program with specific focus on security and privacy matters.
9. Recommend method of vulnerability detection and mitigation and oversee vulnerability testing and reporting.
10. Serve as AHDB's contact point for auditors and government on information security and privacy matters.
11. Maintain knowledge of latest security and privacy legislation, regulations and standards.
12. Participate in Business Continuity Planning and Disaster Recovery planning as required.
13. The post holder will also be expected to carry out any other duties that may be reasonably requested by the IT Manager including deputising for the IT Manager if required.

KNOWLEDGE / EXPERTISE / MINIMUM QUALIFICATIONS

- Graduate level.
- Information security management qualification (eg. CISSP, CISM)
- Knowledge and experience of developing and implementing information security policies, procedures, standards and guidance.
- Experience in developing and administering an information security program.
- Knowledge of statutory and regulatory requirements.
- Knowledge and experience of implementing industry best practice standards (eg. ISO 27001).
- Technical awareness in the areas of IT architecture, development and operations.
- Project management skills and experience.
- Excellent communication and presentation skills.
- Good administration and planning skills.

OTHER ATTRIBUTES / KEY SKILLS/COMPETENCIES

SIGNATURE (Post holder):

DATE:

SIGNATURE (Manager):

DATE: