Principles for Information Security Practitioners

A Support the business		
PRINCIPLE	OBJECTIVE	DESCRIPTION
A1 Focus on the business	To ensure that information security is integrated into essential business activities.	Individuals within the security community should forge relationships with business leaders and show how information security can complement key business and risk management processes. They should adopt an advisory approach to information security by supporting business objectives through resource allocation, programmes and projects. High-level enterprise-focused advice should be provided to protect information and help manage information risk both now and in the future.
A2 Deliver quality and value to stakeholders	To ensure that information security delivers value and meets business requirements.	Internal and external stakeholders should be engaged through regular communication so that their changing requirements for information security can continue to be met. Promoting the value of information security (both financial and non-financial) helps to gain support for decision making, which can in turn help the success of the vision for information security.
A3 Comply with relevant legal and regulatory requirements	To ensure that statutory obligations are met, stakeholder expectations are managed and civil or criminal penalties are avoided.	Compliance obligations should be identified, translated into requirements specific to information security and communicated to all relevant individuals. The penalties associated with non-compliance should be clearly understood. Controls should be monitored, analysed and brought up-to-date to meet new or updated legal or regulatory requirements.
A4 Provide timely and accurate information on security performance	To support business requirements and manage information risks.	Requirements for providing information on security performance should be clearly defined, supported by the most relevant and accurate security metrics (such as compliance, incidents, control status and costs) and aligned to business objectives. Information should be captured in a periodic, consistent and rigorous manner so that information remains accurate and results can be presented to meet the objectives of relevant stakeholders.
A5 Evaluate current and future information threats	To analyse and assess emerging information security threats so that informed, timely action to mitigate risks can be taken.	Major trends and specific information security threats should be categorised in a comprehensive, standard framework covering a wide range of topics such as political, legal, economic, socio-cultural as well as technical issues. Individuals should share and build on their knowledge of upcoming threats to proactively address their causes, rather than just the symptoms.
A6 Promote continuous improvement in information security	To reduce costs, improve efficiency and effectiveness and promote a culture of continuous improvement in information security.	Constantly changing organisational business models - coupled with evolving threats - require information security techniques to be adapted and their level of effectiveness improved on an ongoing basis. Knowledge of the latest information security techniques should be maintained by learning from incidents and liaising with independent research organisations.

B Defend the business		
PRINCIPLE	OBJECTIVE	DESCRIPTION
B1 Adopt a risk-based approach	To ensure that risks are treated in a consistent and effective manner.	Options for addressing information risk should be reviewed so that informed, documented decisions are made about the treatment of risk. Risk treatment typically involves choosing one or more options, which typically include: accepting risks (ie by a member of management 'signing-off' that they have accepted the risks and that no further action is required); avoiding risks (eg by deciding not to pursue a particular initiative); transferring risks (eg by outsourcing or taking out insurance); and mitigating risk, typically by applying appropriate security measures (eg access controls, network monitoring and incident management).
B2 Protect classified information	To prevent classified information (eg confidential or sensitive) being disclosed to unauthorised individuals.	Information should be identified and then classified according to its level of confidentiality (eg secret, restricted, internal and public). Classified information should be protected accordingly throughout all stages of the information lifecycle - from creation to destruction - using appropriate controls, such as encryption and access restrictions.
B3 Concentrate on critical business applications	To prioritise scarce information security resources by protecting the business applications where a security incident would have the greatest business impact.	Understanding the business impact of a loss of integrity (eg completeness, accuracy and timeliness of information) or availability of important information handled by business applications (ie processed, stored or transmitted) will help to establish their level of criticality. Security resource requirements can then be determined and priority placed on protecting the applications that are most critical to the success of the organisation.
B4 Develop systems securely	To build quality, cost-effective systems upon which business people can rely (eg that are consistently robust, accurate and reliable).	Information security should be integral to the scope, design, build and testing phases of the System Development Life Cycle (SDLC). Good security practices (eg rigorous testing for security weaknesses, peer review and ability to cope with error, exception and emergency conditions) should play a key role at all stages of the development process.

C Promote responsible security behaviour		
PRINCIPLE	OBJECTIVE	DESCRIPTION
C1 Act in a professional and ethical manner	To ensure that information security-related activities are performed in a reliable, responsible and effective manner.	Information security relies heavily on the ability of professionals within the industry to perform their roles responsibly and with a clear understanding of how their integrity has a direct impact on the information they are charged with protecting. Information security professionals need to be committed to a high standard of quality in their work while demonstrating consistent and ethical behaviour and respect for business needs, other individuals and confidential (often personal) information.
C2 Foster a security-positive culture	To provide a positive security influence on the behaviour of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.	Emphasis should be placed on making information security a key part of 'business as usual', raising security awareness amongst users and ensuring they have the skills required to protect critical or classified information and systems. Individuals should be made aware of the risks to information in their care and empowered to take the necessary steps to protect it.