REQUIREMENTS	SCOPE OF APPLICABILITY	Notes
'Top-level' security policy	Organisation-wide	One-two page document
Information security policy		Included business impact assessment undertaken from the Confidentiality, Integrity and Availability perspectives.
Change control procedure		
Security handbook		
Incident management procedure		
Disciplinary procedure		
Backup & archiving policy		
Monitoring & audit policy		
Risk Management & Accreditation Document Sets (RMADS)	Systems and networks operated by the organisation	Developed by CLAS consultant in accordance with Infosec Standard No. 2.
Risk assessment and/or Gap analysis		Infosec Standard No.1 A risk assessment provides the justification for recommending security requirements.
ICT administration procedure & work instructions (as appropriate)		
Third-party & Outsourcing contracts		Templates for contracts with third party organisations.
Operating procedure, SyOps or 'Acceptable usage' policy		Short document describing the responsibilities of key role holders, e.g. user, system security officer, IT manager. Supported by awareness training (on an 'on-going' basis)
Authorisation procedure for access to networks, systems and/or applications.		
Security review and testing procedure		IT security health checks Review of access control lists Interviews with stakeholders Review of logs and control sheets
Codes of Connection		Describes the security requirements that need to be addressed in order to connect to a network.