

## **Information Access and Security Policy**

### **Appendix 2 - Technical Procedures**

*In order to support the implementation of the Information Access and Security Policy, procedures will be maintained in the areas listed below. Where procedures exist already they will be reviewed in order to determine if they meet needs; where procedures do not exist they will be developed; all procedures will be reviewed regularly and the implementation of procedures will be subject to regular audit*

<b>Area</b>	<b>Procedures</b>
User Registration	Registration for general computing facilities
	De-registration procedure
	Password recommendations
	Authentication
Network Facilities	Registering & security of network devices
	Nomadic network
	Remote access
	Remote proxy
	Intrusion incident handling: <ul style="list-style-type: none"><li>- Network</li><li>- Unix/Linux</li><li>- Windows</li></ul>
	Firewall
	Personal firewalls
Systems Security	Systems administration <ul style="list-style-type: none"><li>- patching</li><li>- secure connections &amp; encryption</li></ul>
	Anti-virus
Backup	Central data
	Departmental data
Information Assets – Inventories	Central Assets <ul style="list-style-type: none"><li>- Unix/Linux hardware</li><li>- Windows hardware</li><li>- Network hardware</li><li>- All Software</li></ul> Corporate:Data Departmental Assets
Central Systems configuration management	Network facilities UNIX servers Windows servers Database/web Library systems Corporate Applications

Information Access Control	Corporate Data:
	Database Administration
	Regular review of access rights
	Third party access control
	Test data anonymisation
System privileges	Authorisation
Disaster Recovery/ Business Continuity	Disaster Recovery
Physical Security	Computer rooms Networks Personal computers – Security & Disposal
Audit	Policy audit Vulnerability testing