Security Risk Log

Amanda UNIX backups

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to backup servers	Servers kept in a secure location.	CMP Support	Low	High	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Backup tapes damaged or lost	Tapes held in fire safe, multiple backup sets kept.	CMP Support	Low	Low	05/11/2010	Acceptable risk

CMP Active Directory

Authentication and Authorisation

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorized use of Domain Admnistrator account	Use secure password (as per SM5.3.1). Restrict knowledge of account password to authorised users. Change regularly or when authorised staff member leaves (as per SM5.3.3)	CMP Support	Low	High	05/11/2010	Acceptable risk

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to Domain Controllers, leading to possible security attacks	House servers in secure location (CMP Machine Room). Majority of systems now migrated to central AD service, final system to be removed before next review.	CMP Support	Low	High	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale

Data corruption of Directory Service	Daily backups of Domain Controller system state. Resiliance through multiple domain controllers. Regular disaster recovery tests.	CMP Support	Low	High	05/11/2010	Acceptable risk

CMP Publication system

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Loss of data in the schools publication system	Nightly backups taken and plans to migrate to the new system when it become available	CMP Support	Low	Medium	05/11/2010	Within 1 year

CMP Website

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to webserver	Server located in secure area. Majority of content has been migrated to the CMS.	CMP Support	Low	High	05/11/2010	Within 1 year

DHCP

Network Infrastructure

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
DHCP broadcast spoof attack	Long static leases to client PCs.	CMP Support	Low	Low	05/11/2010	Acceptable risk

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to servers.	Servers held in secure location. Service spread across multiple systems.	CMP Support	Low	Medium	05/11/2010	Acceptable risk

DNS

Network Infrastructure

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
DNS poisoning	Zone transfers restricted. Dynamic updates disabled. Plan to migrate service to central DNS service.	CMP Support	Low	Medium	05/11/2010	Within 1 year

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to servers.	Servers held in secure location. Service spread across multiple systems.	CMP Support	Low	Medium	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Data corruption to DNS zone information	Daily backups by Amanda service	CMP Support	Low	High	05/11/2010	Acceptable risk

FlexLM

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to server	Server virtualised. Host server kept in secure location.	CMP Support	Low	Low	05/11/2010	Acceptable risk

Linux Computers

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to PC	Computers kept in locked research labs. Students advised to ensure physical security of the areas they use (windows/doors locked etc)	CMP Support	Medium	Low	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale

Theft of information from Linux based laptops	Disabling of booting from alternative devices. Research into suitable full disk encryption required and supporting infrastructure	CMP Support	Low	Medium	05/11/2010	Within 1 year

Macintosh Computers

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to PC	Computers kept in locked research labs. Students advised to ensure physical security of the areas they use (windows/doors locked etc)	CMP Support	Medium	Low	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Theft of information from Machintosh based laptops	Enforcing UEFI passwords to boot from alternative devices. Research into suitable full disk encryption required and supporting infrastructure	CMP Support	Low	Medium	05/11/2010	Within 1 year

Postgraduate Desktop

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to PC	Computers kept in locked research labs. Students advised to ensure physical security of the areas they use (windows/doors locked etc)	CMP Support	Medium	Low	05/11/2010	Acceptable risk

Postgraduate Laptop

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to system	Students advised to keep laptops in secure areas and use Kensington locks where possible. Students expected to be responsible for the physical security of their equipment at all times.	CMP Support	High	Low	05/11/2010	Acceptable risk

Retrospect Backup

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to backup servers	Servers kept in a secure location.	CMP Support	Low	High	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Interception of backup data	Client/Server security enabled for all clients	CMP Support	Low	High	05/11/2010	Acceptable risk
Backup tapes damaged or lost	Tapes held in fire safe, multiple backup sets kept.	CMP Support	Low	Low	05/11/2010	Acceptable risk

Staff PC

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to PC	Computers kept in locked offices. Staff advised to be aware of physical security at all times.	CMP Support	Medium	Medium	05/11/2010	Acceptable risk

Storage and Data Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Data corruption leading to loss of work	Systems backed up with Retrospect backup software	CMP Support	Low	Medium	05/11/2010	Acceptable risk
Theft of information from Windows based laptops	Disabling of local accounts with administrator privileges, disabling of booting from alternative device. Move to full disk encryption when relevent infrastructure in place	CMP Support	Low	Medium	05/11/2010	Within 1 year

Stuweb Teaching Service

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised physical access to servers.	Servers held in secure location.	CMP Support	Low	Medium	05/11/2010	Acceptable risk

Undergraduate Labs

Physical Security

Risk	Mitigation	Owner	Likelyhood	Impact	Last Reviewed	Timescale
Unauthorised removal of PC equipment	Secure PC and Monitors as per SM3.1.5	CMP Support	Low	Low	05/11/2010	Acceptable risk