BIO IT Risk Log – ISC10D014

Information Technology Risk Log

The risk log contains all risks that have been identified. Explanations of the fields in the risk log are outlined below. The purpose is to provide a repository of information about risks, their analysis, countermeasures and status

No	Description	Likelihood	Severity of Effect	How is risk being managed/mitigated	Owner	Date (if applicable)	Impact Area
01	Phishing scam prevention – staff password security	M	H	Forewarning and advice on current threats. Emails go out to staff to avoid them when threat identified, web page for further info.	BIO IT	July 2007	I,G,R
02	Data Security - servers	M	H	Backup server data to central file store. DRP for reinstatement	BIO IT	24/07/09	G,EUEA
03	Data security – workstations/ users	M	H	Encourage users to store data on central file store	BIO IT	24/07/09	G,I
04	Non standard equipment	M	H	Specialist scientific equipment / facilities checked for non compliance of university IT policies. Measures taken to comply where possible.	BIO IT	Jan 09	G,I
05	Server Hardware failure	M	M	High level of hardware redundancy RAID systems and UPS plus 4 hr response maintenance for critical services	BIO IT	24/07/09	G,EUEA
06	Unauthorised data access	M	H	Control network share or Web access of data by AD user or Groups. Use local accounts on non AD dedicated scientific equipment	BIO IT	Sept 2008	G
07	Unauthorised disconnection of servers from network	L	H	Servers in secure area , limit access to authorised persons	BIOIT / ITCS	24/07/09	G, EUEA
08	Unauthorised physical access to servers	L	H	Housed in secure area, limit access to authorised persons, cases locked.	BIOIT / ITCS	24/07/09	G, EUEA

09	Design of specialist facilities	M	H	Assist in grant applications to ensure current standards of data security and equipment specification are adhered to.	BIO IT	2008	I,G,EUEA,P
10	New software updates	M	H	Ensure all users are kept informed when software is distributed.	Individual Users/BIO IT		G
11	New (uea) Operating system Rollout	H	H	Loss of data, install individually to users when requested within the time limit.	BIOIT		C, P
12	Uea IT policies for New PG's	M	M	PG Students are not aware of policies and procedures. Inform students in introductory talks	FITSM	Sept 2007	C
13	User local admin rights on PCs	L	L	Used for installation of software/hardware. User has temporary admin rights to install software.	BIO IT	14 Oct 2010	P
14	Network card failure	L	H	Provide another PC / laptop until network card is replaced	BIO IT		I
15	Virus attack prevention	L	H	Keep all PCs updated with Anti Virus software; advise all users to keep laptops up-to-date and how to scan documents/email.	BIO IT	Oct 2008	I,C, P

BIO IT Risk Log – ISC10D014

Key to Risk Log:

Risk number allocated

Unique identifier for each item in risk log.

Description

Summary of risk

Likelihood of occurrence

Provides an assessment on how likely it is that this risk will occur. Classifications are: L-Low(<30%) , M-Medium (31-70%), H-High(>70%).

Severity of effect

Provides an assessment of the impact that the occurrence of this risk would have on the team L-Low(<30%) , M-Medium (31-70%), H-High(>70%).

How is risk being managed / mitigated

Action to be taken to prevent, reduce or transfer the risk. This may include production of contingency plans.

Owner

Individual responsible for the ensuring this risk is appropriately managed and counter measures are undertaken.

Date identified

Record of when risk was identified.

Impact Area

B = budget	C = Communications	EUEA = External to UEA
P = Plan	R = Reputation	EP = External to project, but within UEA
Q = Quality	G = School/Dept	I - Individuals