Third Party Information Security Questionnaire

This questionnaire is to be completed by the system administrator and by the third party hosting company if a separate company is used.

Name:	
Position held:	
Company Name:	

Is your organisation ISO27001 accredited:	If yes please provide a copy of your current certificate

1. What Information Security training is given to employees, relevant contractors and third party users?	
2. What security checks are made on employees prior to commencement of employment?	

3. What Information Security policies do you have in place? Please provide copies, and confirm whether your users are required to sign an Acceptable Use declaration.	
4. What is your company policy for password formation in respect of the following and how is it enforced? 1) Password minimum length/complexity 2) Password change interval 3) Password history 4) Account lockout (after invalid password entries) Is a screen lock enforced after a set amount of user inactivity?	
5. What disaster recovery and business continuity policies and procedures do you have in place? Please provide copies.	

6. What is the process for notifying customers if their data has been compromised?	
7. What are your company's backup procedures including frequency of the backups, the retention schedule and the storage location of backup media?	
8. What hardware based firewalls do you have in situ protecting your internal network?	
9. What network Intrusion Detection or Intrusion Prevention Systems do you have installed?	

10. What is the process for applying OS and Software security updates to your company's PCs and Servers? Please state if updates and patches are tested before being applied. Is the process documented?	
11. What process and procedures are applied to remove unnecessary services from running automatically on operating systems?	
12. Are all pre-installed system account passwords changed from their defaults on your internal systems?	
13. What Anti-Virus solution(s) do you have installed on your servers, filers and desktops? What is your policy for the application of updates?	

14. What personal firewalls do you have installed on your company's devices?	
15. What email anti-virus solution(s) do you have at the gateway and on the email servers?	
16. Do you commission penetration testing on your organisation's networks and ICT systems? What is the frequency of the testing? Is the testing carried out by independent CLAS,CHECK or CREST accredited testing providers?	
17. What SSL/TLS encryption is used to protect data in transit?	

18. What methods are used if data needs to be transferred physically? How is the data secured in transit?	
19. If wireless connectivity is deployed within your network what wireless security mechanisms do you have in place?	
20. What is your policy for the use of laptops and other mobile devices? Please include the security mechanisms applied e.g. encryption and two factor authentication.	
21. What is your policy for the use of removable media such as memory sticks and CD/DVDs? Please include the security mechanisms in place such as encryption	

22. Please detail the physical security implemented at your data centres. Information to include: 1) Manned guarding 2) Electronic Surveillance 3) Intruder Detection Systems 4) Access Control Systems 5) Recording of access 6) Locks on windows, cabinets and doors.	
23. Please detail the specification of servers used for hosting customer services or processing customer data including the encryption in place.	
24. What technical and organisational measures do you use to restrict and regulate your employee's access to customer's data?	

25. Is there auditing of your employee's access to customer's information systems? If so what is audited? E.g. changes made, failed access attempts etc.	
26. If there is auditing in place what is the retention schedule for the audit logs?	
27. What is your policy for the secure disposal of hardware and media containing customer data (e.g. back-ups, print outs, tapes etc.)?	
28. Where subcontractors provide any service as part of the ICT solution, the provisions in place with the subcontractor(s) ensure that the same levels of protection can be guaranteed in regard to data security.	

Section 2: Personal Data security questions

The following questions are for systems that will process and/or store personal data.

29. Please give details of your data protection infrastructure (including any policies and procedures)	
30. Who is the person within your company responsible for data protection?	
31. Please give your ICO Registration Number.	
32. What training do your employees receive in data protection and confidentiality?	

33. Please provide evidence that a breach of the data protection act is a disciplinary offence within your organisation (e.g. condition of contract etc.).	
34. Are any of the servers that will be used to host university data located outside of the EEA? If so where are they located? If they are outside of the EEA please detail any agreements that are in place.	
35. If Sub Contractors are to be used what mechanisms will be in place to ensure that the same levels of protection can be guaranteed where the sub-contractor has access to personal or sensitive data?	