OUTSOURCING / EXTERNAL HOSTING SERVICES
Security Checklist

The Outsource / External Hosting Services security checklist applies
to situations where Cleveland State University is considering an

Outsourcing or Hosting Services Security Checklist

Section to be completed by Hosting Provider **Please provide a Yes, No or N/A to each question. If a question is answered with a No or N/A, please provide additional information in the Comments section.**				
	Yes	**No**	**Comments**	

a. Does co-location facility provide physically secure "apartments" or cages for each tenant's equipment?			
b. Is the server racks/cage area locked?			
c. Are the servers kept in an area with access restricted to authorized personnel?			
d. Are monitoring and surveillance solutions implemented?			
13. Are servers protected by environmental controls (smoke detectors, fire suppression systems, water sensors, uninterruptible power supplies (UPS), and temperature sensors?			
14. Are all visitors required to sign a security log and be accompanied by an escort while in production areas?			
15. Does your organization have an Information Security Administrator function separate from a System Administrator function?			
16. Are external audits performed on the physical and information security controls? How often?			
17. When was the last audit performed?			
18. Can a copy of your most recent external audit report be provided to Cleveland State University for review? (i.e. SAS70-Type II report, external audit report and/or executive summary of audit) ** For PCI, please include documentation showing a recent PCI audit			
19. Do you log unauthorized attempts to the system and application?			
20. Do you preserve event logs in case of a breach or investigation?			
21. Are logs kept in a central location, separate from the system components?			
22. How long are logs retained?			
23. Does your organization use a local Intrusion Prevention System(s) IPS?			
24. Does your organization use a local Intrusion Detection System(s) IDS?			
25. Are procedures in place for reporting and responding to possible security incidents?			
26. Do you have a separate development environment from your production environment?			
271. Is there a separate test environment?			
28. Are documented change control procedures in place?			
29. Are logical security measures in place to protect Cleveland State University's data from modification, disclosure, and destruction?			
30. Will Cleveland State University data be securely segregated from the data of other customers?			
31. Will encryption be used on any of Cleveland State University data? If YES, please indicate the encryption to be used and where in the *Comments* field.			

Provider Information:	
Completed By:	
Title:	
Date:	
Contact Information:	