OUTSOURCING / EXTERNAL HOSTING SERVICES
Security Checklist

April 2011

The Outsource / External Hosting Services security checklist applies to situations where Cleveland State University is considering an external hosted service such as an application service provider (ASP) or a software-as-a-service (SaaS) provider.

Applications and services hosted by externally hosted services bring special security challenges. Some challenges presented are system and application patch management, network protections, privacy and protection of University data, incident response, data backup and disaster recovery procedures.

The ability of Cleveland State University to service its students, manage its costs and meet its regulatory requirements may be affected by the products, services and systems that are hosted by third party providers. In selecting a host provider, it is important to take into consideration many factors, such as strategic purpose, business objectives, risks, benefits, legal requirements, costs, needs, financial stability, performance capabilities and technical and operational requirements.

This checklist is a guide for evaluating the security of an external hosting service that will be providing hosting services for University information.

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**
1. Does your organization have a documented and provable internal information security policy in place that details your information protection program for both logical and physical security? (List of items in security policy: organization structure, physical security, hiring and termination procedures, data classification, access control, operating systems, Internet use, e-mail, virus protection, firewall, VPN, remote access, backup and disaster recovery, personnel security, software development)			
2. Is this policy reviewed and updated on a regular basis?			
3. May a copy of your information protection program be reviewed by Cleveland State University's IS&T Department, Purchasing, Audit and Legal? An RFP process should be followed if required by State rules.			
4. In order to protect the confidentiality, integrity and availability of Cleveland State University's confidential information, does your organization ensure that:			
a. Information and services are provided only to those authorized?			
b. Information is protected so that it is not altered maliciously or by accident?			
c. Information and services are provided in conjunction with the vendor's disaster recovery and business continuity planning policy?			
5. Is there a redundant site in another location your organization utilizes in the event of a disaster/failure?			
6. Are backup / recovery procedures updated and tested annually?			
7. What type of testing do you conduct for your business continuity and disaster recovery plan (i.e. simulation drills, walk-through exercises, tabletop exercises, actual drills, etc.)?			
What is the frequency?			
8. How long do you estimate it will take to restore a product or service should you experience a serious business interruption that lasts more than 1 business day?			
9. Is access to offline media and backup data restricted to authorized individuals only?			
10. Are physical security measures in place to protect Cleveland State University data from modification, disclosure, and destruction?			
11. Does your organization use a co-location facility for housing your servers?			
12. If a co-location facility is used:			

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.			

32. Who will have access to Cleveland State's data?			
33. When are they authorized to handle/view our data?			
34. Who will handle the administration of the users in the application?			
a. Cleveland State University			
b. Provider			
35. Does your organization enforce a strong password policy?			
36. Are your employees/contractors required to sign a confidentiality agreement?			
37. Do you have a mandatory security awareness program in place for employees to make them aware of confidential information, the company's security policies and standards and good security practices?			
38. Are reviews conducted to validate that user access is			

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