

Application Development within University

Security Checklist

The Application Development using data from the University Enterprise Systems or application Development for departmental use security checklist for Cleveland State University.

Applications and services developed internally bring



Application Development - Security Checklist

Section to be completed by Developing Department 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. In order to protect the confidentiality, integrity and availability of Cleveland State University's confidential information, does your Department ensure that:			
a. Information and services are provided only to those authorized? PeopleSoft data access should be provided following CSU access approvals.			
b. Information is protected so that it is not altered maliciously or by accident?			
2. Who will have access to Cleveland State's data?			
3. Who will handle the administration of the users in the application?			

4. Are reviews conducted to validate that user access is appropriate? (i.e. inactive accounts, employees who have changed
aiyom emmm

eamaa14(t)1d [(5()JTJ93067(a)3.7930694)3.79306()-5.563895()q4

10. Can your application leverage existing enterprise authentication mechanisms (eg: LDAP, Kerberos, etc.)?			
11. Change Control process for CSU Administrative Systems must be followed for all applications developed using CSU Enterprise system data and should be used for developing other applications for the University.			
12. Do you have a separate development environment from your production environment?			

13. \$.36.6.99 | 4288 8805.99 | 4116 8805.99 | 4116 8915.99 | h W* n /R41 c78]TJ -219.228 -10.44 T8.T78l h W* n .315738(9 r4069 894.6547(o)-3.97114(p.228re f 3



23. Will encryption be used on any of Cleveland State University
