Application Development within University

Security Checklist

April 2011

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 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 development of applications using CSU's Enterprise data and then managed by various departments on campus. In developing applications using CSU data; 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 as well as security.

Applications developed using CSU Enterprise Systems and data must follow the University IS&T development protocol and are required to have IS&T oversight. Applications being developed that do not use CSU systems and or Enterprise data must also follow University policies for development and security.

This checklist is a guide for evaluating the security of the application being developed and a review of the development process for conformity with CSU requirements.

Application Development Risks

Application

The application cannot be supported by IS&T. Since the application was developed by resources outside of the IS&T Department, IS&T will not have any knowledge of the application code nor any database structure supporting it. Should the resource that developed the application leave your department the application may become unreliable. If a user base has become heavily reliant on the application then a serious problem could result in the event it no longer functions.

Upgrades and modifications to the enterprise systems may break external applications. System updates, weather through cyclic upgrade or modification due to business necessity, may change the data structures, network location, or other elements that are key to an external application.

Upgrades in desktop operating systems may impact the applications performance or some of its functionality. The resource responsible for the development must be prepared to manage these changes.

Data

Anytime data is extracted from the primary enterprise data base and loaded to another to be used for an independent application there is always a risk surrounding data integrity. The university's enterprise data base is the official source for institutional data.

If the enterprise data base is the source of the data then whenever an upgrade to the enterprise system occurs it may require modifications to the local application data base.

The data for whatever reason becomes corrupt or inaccessible. If there is no formal procedure to back up the data stored in the local application data base, recovery could be difficult if not impossible.

Security

Data stored locally on equipment within the department is at risk of loss from theft, unintentional / intentional damage or any number of environmental threats (eg. Heat, water etc.).

External applications proxy authority. Applications using enterprise data but which provide their own authentication schemes bypass the procedural controls if not properly implemented.

Regulatory adherence. External applications can expose the University to liability by unintended exposure that violates FERPA/HIPAA, or by allowing the appearance of discrimination.

Portability. Careful attention must be paid to interfaces (proxied or otherwise) to enterprise data via mobile devices.

Logging. Transaction logs created by independent applications are not centrally stored, and can be altered or unavailable to assist in a forensic investigation in the event of a security incident. Proxied authority enhances this risk (the forensic trail will likely end within the department, possibly to the individual developer who is extracting the data from the enterprise application).

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 job responsibilities or who have terminated employment)			
What is the frequency? (Monthly, Quarterly, Semi-annually, Annually)			
5. Do you immediately disable or modify access entitlements when an employee's status changes (termination, transfer, etc)?			
6. Is there a documented process to verify a requestor's identity and the need-to-know before access is given to Cleveland State University information?			
7. Do you have a mandatory security awareness program in place for employees to make them aware of confidential information, the University's security policies and standards and good security practices?			
8. What devices and methods will be used to access the application and/or data?			
a. Defined CSU workstations (wired, static IP)			
b. Non-defined CSU workstations (campus wide)			
c. Public (Internet facing) access			
d. Mobile devices (phones, tablets, etc.) [requires special consideration if (c) is excluded]			
9. Does the application log access attempts (success and failure)? Where does logging occur, and what mechanisms are present to prevent alteration?			

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. Are documented change control procedures in place?			
14. Are backup / recovery procedures updated and tested annually?			
15. How long do you estimate it will take to restore a product or service should you experience a serious interruption that lasts more than 1 business day?			
16. Is access to offline media and backup data restricted to authorized individuals only?			
17. Are physical security measures in place to protect Cleveland State University data from modification, disclosure, and destruction?			
18. If a server is not located in the University Data Center:			
a. Does department location provide physical security?			
b. Are the servers kept in an area with access restricted to authorized personnel?			
c. Are monitoring and surveillance solutions implemented?			
d. Are servers protected by environmental controls, smoke detectors, fire suppression systems, water sensors, uninterruptible power supplies (UPS), and temperature sensors?			
19. Are procedures in place for reporting and responding to possible security incidents?			
20. Are logical security measures in place to protect Cleveland State University's data from modification, disclosure, and destruction?			
21. Is the application behind the CSU firewall? (Lanyard)			
22. Will Cleveland State University data be securely segregated from the data of other applications for the College or Department?			

23. 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.			
24. Are procedures in place for reporting and responding to possible security incidents?			
25. Do you apply security patches on a regular basis? If YES, please indicate the frequency in the *Comments* field.			
26. Do you have a defined process for testing and applying critical patches outside of your regular patch cycle?			
27. Is the appropriate anti-virus software employed and regularly updated?			
28. Are external audits or internal audits performed on the physical and information security controls? How often?			
29. When was the last audit performed?			
30. Do you outsource any processing to another third party provider?			
If Yes, list the names of outsource provider(s).			
31. If outsourcing is done, have you determined that the security policies of the provider comply with your own? If CSU data is being hosted by an outside provider or is being stored by an outside provider please have the Third Party Hosting Security Checklist completed by the company. It can be found on the CSU Purchasing Web site.			

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