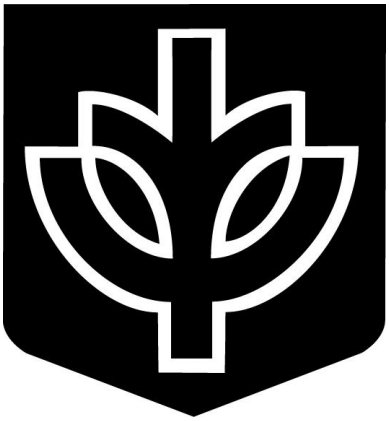
INFORMATION AND DATA SECURITY CLASSES



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604 US
https://infosec.depaul.edu/

18th December 2002

Copyright Notice

Contents

1 Summary

Modern computer data and information management technologies allow organizations to promote the use of the Internet for business processes. DePaul University has chosen the Internet as a medium for allowing students, faculty and staff to access resources including financial statements, enrollment preferences to various programs, and more.

With the wealth of resources offered by the University also comes the risk of malicious acts that disclose, modify, add or destroy sensitive and confidential data. In any instance involving these acts, the University may be held liable to various local, state and federal guidelines governing the secure use of personal data.

This document recommends classification of information, data and the applications and systems that store and distribute such content. When building new applications, or securing legacy systems, we *strongly recommend* you review this policy and apply it as necessary to such situations.

2 Security Classes

The system defined in this document relies on three (3) security class levels for defining data. These classes are:

- **Public**: Information defined as public information, whether in the form of data, documents, source code, applications, or any other medium, *should not* include any of the following types of data.

  1. Business plans, strategies or development goals not specifically intended for public disclosure.
  2. Financial information of the University, students, faculty or staff.
  3. Student, faculty and staff demographic data.
  4. Risk assessment and internal audit information.
  5. Details detailing core infrastructure technologies and configurations.
  6. Internal communication [1] and communicaiton between University consultants, partners and service providers or other similar parties.
  7. Policies and procedures not implemented University-wide or those policies and procedures that, if disclosed, could compromise the security of the University, in part of whole.
  8. References to information and data contained in higher security classes, including sensitive and private information classes.

  Public class information may often be found on World Wide Web (WWW) servers allowing anonymous access, File Transfer Protocol (FTP) servers allowing anonymous access and in public messaging forums such as USENET groups, mailing lists, etc.

- **Sensitive**: This security classification *should not* include the following types of data.

  1. Business plans, strategies or development goals not specifically intended for public disclosure.
  2. Financial information of the University, students, faculty or staff.
  3. Student, faculty and staff demographic data.
  4. Risk assessment and internal audit information.
  5. Policies and procedures not implemented University-wide or those policies and procedures that, if disclosed, could compromise the security of the University, in part of whole.
  6. References to information and data contained in higher security classes, including private information classes.

[1] These methods of communication can be in various forms including memo, electronic mail, intranet web sites, messaging, etc.

Sensitive information is found often on the following media: Interorganization electronic mail, office white boards, WWW forums requiring authentication.

- **Private**: Such information encompasses all information discluded from both public and sensitive security classes. Private information *should only* be exchanged by the following methods.

  1. Servers protected by strong authentication methods [2].
  2. End-to-end communication channels over high-grade encryption [3].
  3. Voice communications [4] encrypted with approved devices.

[2] Biometrics, hardware and software tokens, asymmetric encryption keys and other methods explicitly approved by INFOSEC

[3] At the time this document was published, we recommend a *minimum* of 128-bit encryption

[4] Over legacy public switched telephone networks, voice over IP, etc.

3 Implementing Security Classes

Implementing these guidelines requires *all components* of an application or system to be designated into a security classification. To successfully implement a class system, each bit of information *must* be accounted for in a unique class level. A class system specific to security *will not* successfully function in part.

The life cycle of a project starts during the initial development cycle. At this point the class system used for data security (whether it be this system or a similar one) should assist in building the development environment, generate security roles, define migration procedures, etc.

Data in a development environment *should* undergo rigorous security measures and be protected by a defense-in-depth security methodology [5] This security should then be replicated to test, quality assurance and production environments. Production *should not* be used in the development, test or QA environments. False data *should* be substitued when production requirements are not being filled. The audit procedures of false data in development, test and QA environments should be stringent enough to satisfy production requirements.

4 Custom Security Classes

This document may be used, without modification, to assist in securing applications and computer systems. INFOSEC recommends the use of these or other customized, similar, guidelines be applied to all resources supporting current services.

[5] A defense-in-depth system utilizes many layers of security to protect assets. These layers include access control measures through network and host firewalls, layered authentication using unique ID per individual, and “real-time” attack analysis and alerting mechanisms.