

University Declaration of Sensitive Information

Appendix C, to *Information Security Guidelines, Part I, Campus Programs & Preserving Confidentiality*, Document #6608.

Responsible Office: Administrative Services and Technology

February 1, 2008

The University declares the following categories of information to be “Sensitive Information” as defined in Procedure #6608, *Information Security Guidelines, Part I, Campus Programs & Preserving Confidentiality*. These categories, therefore, are to be included in campus declarations of “Sensitive Information” and handled in campus Programs as described in the Procedure.

This listing also contains categories of information that the University *recommends* for campus consideration, these being clearly identified by heading.

I. Confidentiality

The following categories require controls for protecting appropriate use and disclosure:

I.A. Defined in Law

-Applying to All Campuses

1. *personal information* as defined by the NYS Freedom of Information Act (FOIL).
2. *personal identifying information* as defined by the NYS Information Security Breach and Notification Act, and the NYS Disposal of Personal Records Law.
3. *personal information* defined in the NYS Personal Privacy Protection Law and in the related University policy.
4. *personally identifiable information* on students in education records as defined in the Family Educational Rights and Privacy Act (FERPA).
5. *personal information* defined in the NYS Electronic Signatures and Records Act (ESRA).

-Applying to Most Campuses

6. *personally identifiable financial information* on customers in financial lending records as defined in the Gramm-Leach-Bliley Act (GLBA) with its associated Federal Trade Commission Safeguards Rule.

-Applying to a Few Campuses

7. *electronic protected health information*, defined in the Security Standard related to the Health Insurance Portability and Accountability Act (HIPAA).

I.B. Defined in Industry Controls

-Applying to Many Campuses

8. *payment card transaction information* as defined by the Payment Card Industry Data Security Standard (PCI-DSS).

I.C. Defined in University Procedure

-Applying to All Campuses

9. *Personal, Private, and Sensitive Information* (“PPSI”) as defined in New York State’s Information Security Policy (NYS IS Policy).
10. *structural, operational, or technical information* (about electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure) as defined within “PPSI” in NYS IS Policy.
11. *Program Documents* as defined in Document #6608.

I.D. Recommended by the University for Campus Consideration

-Applying to All Campuses

12. *personally identifiable health information* of the type defined by HIPAA yet not technically covered under that law and not restricted to subject (employees, students, alumni, visitors) and not restricted to electronic media.
13. *personally identifiable financial information* of the type defined by GLBA yet not technically covered under that law and of the type defined by PCI-DSS yet not technically covered under that control.
14. *emergency and business continuity plans and operational documents.*

II. Integrity:

The following categories require controls for protecting intended content:

II.A. Defined in University Procedure

-Applying to All Campuses

15. *student records and transcript data* regarding official attendance in University programs (“courses”) and associated assessments of performance and completion of requirements for courses (“grades”) and graduation, and degrees generated by the University.
16. *financial records* regarding official University transactions.

II.B. Recommended by the University for Campus Consideration

-Applying to All Campuses

17. *public University web pages* with significant impact on the public’s understanding and impression of the University’s character, roles, services, faculty, staff, students, and alumni, history, location, buildings, offerings and any other information placed on a University web page that has been reviewed and approved by University management.

III. Availability:

The following categories require controls for protecting intended operational access:

III.A. Recommended by the University for Campus Consideration

-Applying to All Campuses

18. *transactional data and supporting data* necessary to conduct mission-critical transactions in teaching, research, service and administration.
19. *emergency and business continuity plans and operational documents.*