VSC INFORMATION TECHNOLOGY SERVICES

Data Security Practices – November 2, 2005

Information security awareness is an important issue, and one in which every VSC employee must play a role. Most security incidents stem from mistakes made by people who have legitimate access to data. Here are some simple but effective security awareness habits:

1. Remember that you "own" the data in your work area, and you have a responsibility to protect it. When someone asks you for data, ask them:
   - Who authorized the request
   - Why they need it
   - What they will be doing with it
   - Where it will be stored
   - With whom it will be shared
   - When & how it will be destroyed
   - Why they need each data item that they have requested

2. When providing data that contain personal information (for students, employees, or others) do not provide more information than is needed to get the job done. Be especially wary of providing Social Security numbers. The Colleague person ID (a seven-digit number) is the correct way to provide a unique identifier for individuals.

3. We rely on our student workers in every office. At least once a semester, review the roster of student workers. Are they still employed? Has their job changed and does it require a change in their data access? When setting up data access for student workers, do not give them more access than is necessary to do their job, and make sure that they receive security awareness training, including FERPA and how to tell when a student has indicated that personal information is not to be released. Never encourage a student worker to work from their residence hall or somewhere other than the appropriate office.

4. Information security is not just about computers: data exist in filing cabinets, in printouts, on portable drives, and in trash bins. Be aware of these risks to data security, and work with your office and your supervisor to keep data safe.

5. When you leave your computer unattended, lock it or log off. Never disclose your password to anyone. Don't leave your password on a Post-It in your office.

6. Don't store data on the hard drive of your computer or your laptop: use the network storage provided by your college. Never store data on a web drive or other publicly available area.

7. Don't collect data that you don't need or that is already available in Colleague; ideally, all data collected should be stored in Colleague. If you don't know how to do this, please contact your Information Technology department.

8. When you become concerned about a possible security lapse, do something about it! Report it to your supervisor so that the appropriate actions can be taken.

9. Email is no more secure than a postcard! Don't share data files using email. Contact your IT department for secure ways to share files within and outside of the organization. IT should always be involved when sharing data with organizations outside of the Vermont State Colleges.