10 Tips for Website Safety

1. Don't store sensitive data unnecessarily: If there is no longer a need to store a particular file or set of data, delete it or archive to a secure backup.

2. Be mindful of data permissions. Always assume that a file placed on a web server will be viewable by others, likely without any authentication at all to users outside of the organization. Know your data, before posting it publicly.

3. Use the proper tool for the job. Web server space should ONLY be used for files that you intend to share with the public at large. Blackboard and/or Banner/BlazerNET should be used for disseminating grades in a secure manner. Courseware can be stored on public web space. You should also be aware of copyright considerations.

4. Do not use your web space for generic file storage. Private network file shares are available at no cost to faculty for network storage and backups of files that should not be publicly accessible. Department/group shares are also available for files that need to be shared between members of a team or department but not shared with the public at large. Please contact CASIT if you need assistance with establishing a personal or group network share.

5. Information security includes maintaining availability in case of hardware and software failure. Maintain backups of all data that is deemed important to prevent possible loss. CASIT can help with this.

6. Stay on top of security releases: make sure your computer is up to date, any software running in your web space is always patched and up to date, and your anti-virus definitions are up to date. This should happen automatically. If you are in doubt of this, please contact CASIT.

7. Treat security as an ongoing activity. New security threats are always emerging, which means you can't treat your security as a 'do it once and forget about it' task. Be aware of on going security-related issues. Regular audits and security should be ‘top-of-mind’ on a daily basis.

8. Continually learn: take any opportunities you have to learn more. General technology knowledge will help with understanding of more specific and targeted security training. Maintain education on security topics, since the threats are

constantly changing.

9. Information security is everyone's responsibility. Regardless of your responsibilities, if your job involves a computer you should always consider the implications of data security on your day-to-day activities.

10. If in doubt about something computer related, ask. CAS IT is always available to answer any questions that might arise. Issues are better handled up front before there is a problem.