Your information is vitally important to your teaching, research, and scholarship.

If unprotected, your computer is a gateway to thieves and hackers, who can access and modify research data, students’ grades, and other confidential items. Unauthorized access to information could also expose the College to financial and compliance risks. A few simple techniques can help protect your information.

THE DARTMOUTH INFORMATION SECURITY COMMITTEE
INSTITUTE FOR SECURITY, TECHNOLOGY, AND SOCIETY
THE DARTMOUTH CYBER SECURITY INITIATIVE
The number of laptop thefts at Dartmouth has steadily increased since 2008, and laptop and smartphone thefts at airports are also on the rise.

**Encryption**  If it’s confidential and portable, encrypt it. Laptops, netbooks, smartphones, thumb drives, and CDs containing private information can be encrypted. Encryption is fast, easy, inexpensive, and in some cases, already built in to the device (e.g., the iPhone and iPad). Examples of confidential information include research data, students’ grades, evaluations of graduate students, and email. If you are sending confidential information by email, it’s a good idea to encrypt it, especially if the destination is outside Dartmouth. Internet email is not secure, and encryption is the only way to guarantee confidentiality.

**Computer Systems**  Turn off your computer when you are not using it, or configure a screen saver time-out so the computer locks after a period of inactivity. For highly sensitive information, we suggest 15 minutes. This feature can be easily disabled when you are using your computer for presentations.

**Passwords**  Choose a phrase that is easy for you to remember, has no meaning to others, and follows the conventions found at www.dartmouth.edu/comp/systems/accounts/passwords/rules.html. Remember to use passcodes on mobile devices like phones and iPads.

**Paper Documents**  Lock confidential paperwork in desk drawers or filing cabinets. Never leave it on desks or meeting rooms when you are not present. Shred this material when you no longer need it, and discard it in trash bins.

**Web Use**  Be wary of public computers in airport kiosks, libraries, etc. Viruses and key loggers can steal your information. On the Web, look for a lock icon showing a secure connection. If you receive a certificate warning, consider abandoning the connection. Think before you click: phishing attacks are designed to trick you into providing personal information.

**Travel Risks**  Thefts of mobile devices are on the rise, especially in public places such as airports, restaurants, and hotels. Do not store computers and smartphones in checked luggage, and keep a watchful eye on computers when proceeding through airport security. When traveling abroad, keep in mind that certain countries, such as China and Russia, do not permit encrypted devices. You should NOT bring any computers or smartphones containing confidential data to these countries. For information on encryption and travel, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm. If you will be traveling to one of these countries, you should consider bringing a laptop that does not contain any confidential data, and exercise caution when connecting to the Internet, since it is likely your Internet activity will be monitored.

**HOW WE CAN HELP**

The Dartmouth Information Security Committee; the Institute for Security, Technology, and Society; and the Dartmouth Cyber Security Initiative offer the following solutions:

- Whole-disk encryption
- Email encryption (service planned for 2012)
- iPad and iPhone security
- Identity Finder: Computing Services can scan computers to locate personally identifiable information (e.g., SSNs) that should be protected or deleted
- IT consultants to assist with password selection and screen-saver timeout settings

**ADDITIONAL SUPPORT**

**Computing Services**  For technical questions and support, email us at help@dartmouth.edu.

**Records Management**  For advice about the proper disposal of paper documents, contact dartmouth.records.management@dartmouth.edu.

For all other questions about online security, contact:

**Steve Nyman**
Chief Information Security Officer
steven.m.nyman@dartmouth.edu