If unprotected, your computer is a gateway to thieves and hackers, who can access and modify confidential items. Unauthorized access to information could also expose Dartmouth to financial and compliance risks. A few simple techniques can help protect your information.
Key Dartmouth Information Security Policy Requirements:

**Back up your information**
You are responsible to ensure your information is backed-up. Use of the MyFiles service is your best choice to ensure your important data is safe.

**Properly configure devices**
You may use personally owned computers and smartphones; however, these devices must be configured to the same security standards as Dartmouth-owned devices.

**Set a 15-minute time-out**
All computers used to access confidential data, including personally identifiable, health and financial information, must be set with an inactivity timeout feature of not greater than 15 minutes.

**Encrypt and password-protect**
All portable computing devices (including laptops and smartphones) that access or store confidential data, including email, must be password-protected and encrypted.

**Use caution when downloading**
Confidential data may not be downloaded to unencrypted portable media. This includes CDs, USB thumb drives, etc.

**Lock your doors**
Doors to offices containing confidential information, in any form, must be locked after normal business hours.

**Destroy obsolete documentation**
Documents and media containing confidential data which are no longer required must be destroyed.

What you can do:
How to protect your information

**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 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](http://www.dartmouth.edu/comp/systems/accounts/passwords/rules.html) Remember to use passcodes on mobile devices like phones and iPads.

**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.

**Paper documents**

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

**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](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.

---

**A server in a Dartmouth lab was hijacked and used for over 200,000 downloads of botnet malware within 24 hours.**

**The number of laptop thefts at Dartmouth has steadily increased since 2008, and laptop and smartphone thefts at airports are also on the rise.**
How we can help:
Your IT Consultant can help you with the following services:

- Setting up MyFiles for your important information
- Whole disc encryption for portable devices and media
- Email security
- iPad and iPhone security
- Screen-saver timeout settings
- Identity Finder services (locates personally identifiable information your computer)
- Destroying or sanitizing confidential media
- Records Management Office (provides assistance with respect to proper disposal of or archiving confidential paper documents)

About us:

The Dartmouth Information Security Committee

The Dartmouth Information Security Committee (DISC) meets monthly to assess vulnerabilities of information security, and to develop and revise information security policy. All divisions of the College are represented on DISC, which is chaired by Dartmouth’s Chief Information Security Officer.

www.dartmouth.edu/comp/security/resources-security/disc

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