Harvard Central Administration provides critical information and essential services such as payroll, benefits, human resources, directory, and student financial services for Harvard’s community of faculty, staff, and students. Much of this information is confidential and some of it is High Risk Confidential Information (HRCI). High Risk Confidential Information (HRCI) is protected by Massachusetts law. All HRCI users must take care when using this information and must be aware of their obligation to protect it. If you are authorized to work at home using confidential information you must be using a Harvard owned and managed computer with disk encryption installed.

See the list of Do’s and Don’ts on this poster. If you have any questions, please visit www.security.harvard.edu or contact security@harvard.edu.
INFORMATION SECURITY AT HARVARD

DON’T

Store High Risk Confidential Information on your Desktop or Laptop Computer, Cell Phone, or ANY Portable Device

Open SUSPICIOUS EMAIL attachments

Reveal confidential INFORMATION

SHARE PASSWORDS

DO

Understand Harvard security policy and the law
Visit www.security.harvard.edu
Contact security@harvard.edu

Recognize High Risk CONFIDENTIAL Information (HRCI)

Securely remove and destroy HRCI

Obtain CIO APPROVAL to use High Risk Confidential Information

Use a Harvard computer to work with Confidential Information at work and at home

Keep your LAPTOP SECURE

Use SECURE PASSWORDS

Sign a confidentiality agreement annually if required