Every Harvard employee holds the key to securing, protecting, and maintaining the integrity of the University’s high risk information. The new Massachusetts identity theft law mandates reporting of unauthorized acquisition or use of personal information and secure disposal of personal information. The new law also gives each Massachusetts resident the right to place a security freeze on credit reports.

Harvard has developed an Enterprise Security Policy to ensure that Harvard’s technical resources are properly protected, the integrity and privacy of confidential information is maintained, and information resources are available when they are needed. Users of these resources must understand their responsibilities.

www.security.harvard.edu/policy
A new Massachusetts law regarding high risk information applies to you and every other member of the Harvard community.

It Is Your Responsibility To
- Protect high risk information
- Destroy high risk information properly
- Disclose any security breach involving high risk information

Defining High Risk Information...
Name or first initial and last name in combination with ANY of the following in electronic or paper form:
- Social Security number
- Driver’s license number
- State identification number
- Financial account number
- Credit or debit card number
- Biometric indicator such as iris scan info

Harvard’s policy on high risk information applies to you. Every Harvard employee is required to protect confidential or high risk information within the Harvard Enterprise Security Policy. The policy can be found at: http://www.security.harvard.edu/policy

- Protect Social Security number, credit card, or bank account information
- Secure human subject information
- Safeguard personally identifiable medical information
- You should review ANY approved use and protection of confidential information with your local IT director or IT support group

Compliance Responsibility
Each School and Central Administration unit is responsible for the local implementation of these policies under the direction of its CIO or IT Director. Implementation planning, education, training, awareness, and compliance confirmation are the responsibility of the School CIO or IT Director who reports compliance status on an annual basis to the University CIO.

As part of its scheduled review of Harvard’s School information technology areas, Harvard Risk Management and Audit Services (RMAS) reviews each School’s compliance and related education and remediation activities.

Harvard community members may anonymously report areas of concern or non-compliance at http://www.security.harvard.edu/report

Protect Social Security number, credit card, or bank account information
Secure personally identifiable human subject information
Safeguard personally identifiable medical information

If you discover or are dealing with a security breach, you should contact the office of General Counsel by calling 617.495.1280.

A security breach is any unauthorized use, acquisition, or loss of high risk information.