<table>
<thead>
<tr>
<th>Information Security Policy</th>
<th>For Users</th>
<th>For Systems</th>
<th>Research Security Policy</th>
</tr>
</thead>
</table>
| **High Risk Confidential Information** | • Never store high risk information such as SSNs or credit card information on your computer or portable device.  
• Request prior approval from your School CIO if you are working with or outsourcing high risk information. | • Use host based firewalls and install only on private address space.  
• Test systems for vulnerabilities annually.  
• Review remote access arrangements with your School CIO. | 4 |
| **Confidential Information** | • Ensure appropriate controls are in place to protect your information.  
• Use a secure method to transmit your information.  
• Securely lock paper records. | • Implement suitable controls to protect confidential information.  
• Provide a secure file transfer method for users needing to send confidential data. | 3 |
| **Internal Confidential Information** | • Have a legitimate business use for your information.  
• Use internal information only for Harvard business.  
• Acknowledge in Peoplesoft your responsibility for protecting confidential information. | • Prevent malicious traffic from reaching the applications or databases.  
• Employ mechanisms to limit failed logins.  
• Prevent access from the Internet.  
• Keep patch level and virus protection current. | 2 |
| **Public Information** | • Use strong non-shared passwords.  
• Change password if you suspect compromise.  
• Do not store high risk information on your computer.  
• Obtain training suitable for the data you use.  
• Dispose of Harvard Information properly according to law and policy. | • Identify individual users with passwords and enforce password complexity.  
• Prevent passwords from being retrieved.  
• Perform systems administrative tasks only with assigned accounts.  
• Assign extra-complex system administrator passwords  
• Disable default accounts. | 1 |