

Information Security Update



Faculty Senate
February 19, 2009

Randy Livingston, Vice President Business Affairs & CFO

Information Security Task Force

- Formed in June 2008 in response to stolen laptop incident
 - Anxiety among impacted individuals regarding financial impact
 - University mitigation cost > \$1 million
 - Incalculable impact to Stanford's reputation
- Goals:
 - Determine how and why the incident occurred
 - Identify initiatives to reduce the risk of future incidents

Key Task Force Recommendations

● Clarify existing Data Classifications

Prohibited	Restricted	Confidential
<ul style="list-style-type: none"> • Social Security Number • Credit Card Number • Financial Acct Number • Driver's License Number • Health Insurance Policy ID Number 	<ul style="list-style-type: none"> • Protected Health Information ("PHI") • Student records protected by FERPA (allow unencrypted on local computer only as long as necessary but no longer than end of academic year) • Research and other information covered by non-disclosure agreement 	<ul style="list-style-type: none"> • Employment applications/personnel files/personal contact information not contained in a database • Privileged attorney-client communications • Stanford University ID number, internal memos and email, and non-public reports, budgets, plans, and financial information • Non-public contracts

● Disallow storage of Prohibited information on University-owned or personally-owned desktop or portable machines and devices ("Computing Equipment").

● Require encryption when storing Restricted information, and strongly recommend for encryption for Confidential information.

Key Task Force Recommendations

- Use secure email when transmitting Prohibited and Restricted information outside of the Stanford network.
 - Email applications and servers must be properly configured to send information securely on Stanford's email system.
 - Do not use third-party email services, such as Gmail and Yahoo! Mail, as your email account when conducting Stanford business.

Implementation Plans

● Technology currently available:

- File/Folder Encryption – Windows only
- Secure email
 - Voltage Secure Email for messages going outside of Stanford
 - Machines and email servers must be specially configured to send secure email within Stanford if Voltage not used

● Whole Disk Encryption

- Windows and Macintosh expected March 2009
- Linux product in development

Questions & Discussion