Information Security Updates
Senate IT Committee
October 11, 2013
Agenda

• Protecting Sensitive Data
  – What Is Sensitive Data?
  – Available Tools and Resources
  – How CUIT Will Help
  – Pilot of Email Filtering for Sensitive Data (Coming Soon)

• UNI Passwords
  – Guidelines and New Requirements
  – Where to Change Your Password

• Coming Soon
  – IT Security Policy Consolidation and Updates
  – Online IT Security Training
  – Application Risk Assessments
Sensitive Data
Protecting Sensitive Data

• What Is Sensitive Data?
  – Data that is protected by laws or regulations

• Examples of Sensitive Data
  – Protected Health Information (PHI)
  – Personally Identifiable Information (PII)
  – Student Education Records

• How to Protect Sensitive Data
  – Minimize use of sensitive data in files or emails, wherever feasible
  – Encrypt any sensitive data you must send or store
  – Ensure reasonable controls are applied to systems (applications) and to endpoints (e.g., desktops, laptops, mobile devices)
Tools and Resources

• Columbia University Information Security Policies

• CUIT and CUMC Websites
  – Additional Guidelines and Supporting Procedures
  – FAQs and Tutorials
  – Access to Tools

• Support from Your IT Staff
  – Columbia-wide IT Staff Education and Collaboration via IT Leadership Council
  – Help Desk Staff Support
Tools and Resources

• Supporting Tools
  – Encrypting files to be stored or emailed
  – Scanning of workstations for sensitive information
  – Deleting information and sanitizing devices before disposal
  – Monitoring of the network and of emails for abnormal behavior and spam – by CUIT
  – Network scanning of web servers for vulnerabilities or unexpected presence of sensitive data – by CUIT

• Online Security Training (Coming soon)
Encrypting Files – CUIT Documentation and Demo

• How to encrypt? – CUIT online documentation

http://cuit.columbia.edu/cuit/it-security-resources/handling-personally-identifying-information/encryption-tools

• Demo encryption methods
  - Using WinZip
  - Using Microsoft Office
How CUIT Will Help

• Campus-Wide Security Awareness Campaign – Fall/Winter/Spring FY14

• Easier Access to Tools and Support Resources

• Training of Support Staff

• Availability to Talk to Your Departments, Schools, Other Forums

• Monitoring/Detection/Notification of Potential Issues, where Feasible
Pilot of Email Filtering for Sensitive Data

• Heightened awareness campaign
  – Inform users of policies and tools to protect sensitive data

• Blocking of unencrypted emails with SSNs and credit card numbers
  – Block emails if unencrypted sensitive data is detected
  – Notify sender with explanation why email was returned
  – Direct sender to instructions for how to encrypt emails and attachments

• Users will be required to:
  – Put sensitive data in encrypted file;
  – Attach file to email; and
  – Re-send email with encrypted attachment
Phased Pilot of Email Filtering for Sensitive Data

Phasing Over FY14

CUIT – Central Administration – School Administration – Faculty – Students

• Communications to targeted audiences will precede each pilot phase

• Questions or comments are welcomed via email: securityfilteringpilot@columbia.edu
UNI Passwords
UNI Password Guidelines

- Establish password using 8-64 characters
- Include at least three of the following:
  - Uppercase letter
  - Lowercase letter
  - Number
  - Special character (\%\$#@!)
- Do not use your UNI or name as part of password
- Do not choose *commonly used passwords* (e.g. password, admin, 123456)

Recent Study: 90% of passwords are “vulnerable to hacking”
New UNI Passwords Requirements

- Users will be required to change UNI passwords twice a year
- Users will not be able to reuse their last 5 passwords

How will it work?

- **20 days before expiration**: Email reminder to change password
- **10 days before expiration**: At Columbia application login, user will be encouraged to change password
- **After expiration**:
  - User no longer able to log into Columbia network
  - At application login, user will be redirected to password change page

PHASING TO BEGIN THIS FALL
Where To Change Your UNI Password

Real-time Password Self-Service Box

- Helps users enter a strong password
- Immediate feedback
- No need to remember password requirements

uni.columbia.edu
More on Passwords

• Use passwords that are easy to remember, but difficult to guess
  - Passphrases or word combinations

• Other password hints
  - Use a password ring
  - Include some part of the website name in your password

• Beware of Phishing Attacks
  - Always check the domain name in the URL
  - Legitimate companies will not use email to request account information

• Lock your computer and mobile devices
  - Always lock your mobile devices and computer when not in use
Coming Soon
# IT Security Policy Consolidation and Updates

<table>
<thead>
<tr>
<th>#</th>
<th>Revised Policy</th>
<th>Former CU Policy</th>
<th>Former CUMC Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Security Charter</td>
<td>CU Information Security Charter</td>
<td>CUMC IT Security Charter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Security Policy Statement</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Data Classification Policy</td>
<td>Data Classification Policy</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>System Registration and Protection Policy</td>
<td>System Registration and Protection Policy</td>
<td>System Registration and Certification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CUIT Publishing Policy</td>
<td>General Information Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E-Commerce Policy on Credit Card Processing</td>
<td>Information Security: Audit and Evaluation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic Information Server Administration</td>
<td>Information Security: Media, Backup and Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Sanitization Policy</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Endpoint Protection Policy</td>
<td>CU Desktop and Laptop Security</td>
<td>Workstation Use and Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CUIT Security</td>
<td>General Information Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic Information Resources Security</td>
<td>Information Security: Media, Backup and Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Peer-to-Peer (P2P) File Sharing Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Requirements When Storing Sensitive Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>University Mobile Phone Registration &amp; Password Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Sanitization Policy</td>
<td></td>
</tr>
</tbody>
</table>
## IT Security Policy Consolidation and Updates

<table>
<thead>
<tr>
<th>#</th>
<th>Revised Policy</th>
<th>Former CU Policy</th>
<th>Former CUMC Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Social Security Number (SSN) Usage Policy</td>
<td>Social Security Number (SSN) and Unique Person Number (UPN) Usage Policy</td>
<td>None</td>
</tr>
<tr>
<td>6</td>
<td>Network Protection Policy</td>
<td>Network and Communications Equipment Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Bandwidth Quotas</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Information Resources Acceptable Usage Policy</td>
<td>Acceptable Usage of IT Resources</td>
<td>Workstation Use and Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic Information Resources Security</td>
<td>Information Security: Backup, Device and Media Controls</td>
</tr>
</tbody>
</table>
## IT Security Policy Consolidation and Updates

<table>
<thead>
<tr>
<th>#</th>
<th>Revised Policy</th>
<th>Former CU Policy</th>
<th>Former CUMC Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Email Policy</td>
<td>Email Usage and Retention Policy</td>
<td>Email Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Access Policy</td>
<td>Workstation Use and Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Access and Privacy Policy</td>
<td>General Information Security Policy</td>
</tr>
<tr>
<td>12</td>
<td>Sanitization and Disposal of Information Resources</td>
<td>Data Sanitization/Disposal of Electronic Equipment Policy</td>
<td>Information Security: Backup, Device and Media Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic Information Resources Security</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Business Continuity and Disaster Recovery Policy</td>
<td>None</td>
<td>Information Security: Disaster Contingency and Recovery Plan</td>
</tr>
<tr>
<td>14</td>
<td>IRB Data Security Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Online Security Training

• **Initial Scope:**

<table>
<thead>
<tr>
<th>Security Essentials</th>
<th>Protecting Sensitive Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering and Networking</td>
<td>FERPA Basics</td>
</tr>
<tr>
<td>End User Responsibilities</td>
<td>HIPAA Basics (for CUMC / Morningside PHI)</td>
</tr>
</tbody>
</table>

• **Sample Additions:** Columbia IT Policies
Encrypted Sensitive Data

• **Targeted Audience:** All faculty, staff and students

• **Approach:** Voluntary offering to start
HIPAA mandated at CUMC

• **Timing:**
- Late fall 2013 for Morningside campus
- May 2013 for CUMC
Application Risk Assessment

• University-wide Data Risk Assessment
  – Examine legal and regulatory requirements implications for the use and storage of information at Columbia
  – Assess all systems containing sensitive data
    • Protected Health Information (PHI)
    • Personally Identifiable Information (PII)
    • Student Education Records
Application Risk Assessments

How

- Security software system drawing on best practice frameworks to automate, monitor and track risk assessment processes
  - Register systems
  - Conduct assessments
  - Report analysis and findings
  - Track remediation

Scope

- Centralized and decentralized systems at:
  - Columbia University
  - Columbia University Medical Center
  - New York Presbyterian Hospital

Timeline

- CUMC and NYPH systems assessments underway since 2011
- Centralized CUIT systems assessment in process
- Decentralized MS systems registration and assessment to begin FY14 – Q2
Final Comments

Thank you!!