The purpose of this newsletter is to provide the BC community with articles on good business practices, internal controls and responsibilities. Each issue will provide insights to internal control techniques. Additionally, we will provide information on recent items in the news.

We hope that by providing this array of information, we can help you implement effective controls in your area of operations.

Did You Know That…..

Social networking sites can pose as much of a threat as email and website scams. Many people employ social networking websites as a way to steal personal information, especially through phishing. All users of such sites need to be vigilant to protect themselves. Social networks have become an increasingly popular source of information for phishers. They can easily use all of the information stored in your social networking account to steal your identity.

Learn more about phishing at:
http://www.bc.edu/offices/help/security/phishalert.html

Be aware of possible risks, and mitigate potential harm or breach of sensitive data by maintaining up-to-date anti-virus and malware protection software offered by BC Information Technology Services, available at:
http://www.bc.edu/software.

Contents

Social Networking 1
Information Technology Controls 2
General Computer Controls 3
Data Security & The Massachusetts Law 4
In the News 4
Information Technology Controls

Information Technology (IT) controls are specific activities that are designed to ensure business objectives are met. IT controls cover a wide array of processes and apply equally to applications as well as individual employees. Additionally, new technology is always creating challenges for which IT controls must be developed, implemented or strengthened. While IT controls are unable to prevent these occurrences in and of them, they do help to mitigate the risk and severity of these breaches occurring. Below is a summary listing of key IT controls topics for consideration in one's personal and professional life:

• Passwords
  o Strengthen your password by combining letters, numbers and symbols, creating your own acronyms, and changing your password as appropriate. Avoid login names, social security numbers or birthdates, differentiate your passwords, and never store your password on paper.
  o Use a different password for sites where your personal information is stored (i.e., bank, etc.) versus sites where you buy products (i.e., Amazon, etc.).
  o Visit the BC IT Help website for more password tips: http://www.bc.edu/offices/help/getstarted/credentials/pswdtips.html

• Social Engineering
  o Do not divulge confidential information over the phone or via email to others without confirming the requestor's identity and need. Departmental policies can be developed to protect data while maintaining a sense of openness.
  o Contact ITS or your TC upon identification of any suspicious activity.

• Internet & Email Issues
  o Install and maintain virus protection software from BC's website at: http://www.bc.edu/software.
  o Backup all files regularly to ensure business continuity.
  o Do not send chain letters, or participate in pyramid schemes.
  o Remember: Emails have any indefinite life, and are easily retrievable.
  o For information on BC's Email Policy, see http://www.bc.edu/offices/help/comm-collab/email/emailuse.html.

• In and Out of the Office Threats
  o Ensure physical security of all laptops, hardware, and removable media devices (including PDA's).
  o Employ locks, card swipes, and cameras where necessary to prevent unauthorized access to important devices. Don't forget to change locks/combinations when an employee leaves the University.
  o When using wireless internet access, connect to BC's secure wireless network (bcsecure) and avoid public hotspot Wi-Fi connections when viewing sensitive data.
General Computer Controls

General computer controls enhance data integrity by protecting (1) data in transit, (2) stored data on a computer system, and (3) by limiting who can access and modify data. Appropriate information security controls ensure that

- sensitive and confidential data is not compromised or inappropriately shared.
- data is accurate.
- information is available
- the system is reliable.

General computing controls are integrated into policies/procedures and the business objectives of the University. IT audits address the following related control objectives:

<table>
<thead>
<tr>
<th>Audit Trails</th>
<th>Access</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity</td>
<td>Compliance</td>
<td>Data Integrity</td>
</tr>
<tr>
<td>Documentation</td>
<td>Physical Security</td>
<td>Policy/Procedures</td>
</tr>
<tr>
<td>Separation of Duties</td>
<td>System Security</td>
<td>Training/Education</td>
</tr>
</tbody>
</table>

Some enterprise-wide controls include the following tips:

- Define information security policies and communicated them to employees.
- Restrict computer access by job requirements.
- Develop formal procedures for adding, changing, and deleting access to systems including appropriate authorizations and documentation.
- Ensure that the same person does not initiate, authorize, and process a transaction.
- Prepare a comprehensive disaster and recovery plan; test and communicate it to all employees.
- Cross-train staff and executives. Roles and responsibilities should be defined, documented, and communicated to applicable personnel.
- Prepare appropriate documentation to run systems and key programs.
- Actively monitor vendor contracts and re-negotiate as appropriate, including an audit clause.
- Backup data on a regular basis and store off-site.
Data Security and the Massachusetts Law

On March 1, new Massachusetts regulations went into effect requiring institutions to take extra measures to protect the security of personal information of Massachusetts residents (“Massachusetts PI”). Boston College is committed to protecting confidential information, and we are all responsible for creating, using, storing, and destroying data in compliance with federal and state laws.

In light of these new regulations, the University has updated the Data Security Policy at: http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-200.pdf

The Data Security Policy and Massachusetts law requires BC to:

- ensure that confidential information is not accessible to unauthorized people. Confidential information includes Massachusetts PI, which is a person’s first and last name (or first initial and last name) in combination with:
  - social security number;
  - driver’s license or government-issued identification card number; or
  - financial account number (or credit or debit card number).
- make sure, to the extent possible, that any Massachusetts PI is stored only on secure servers or on encrypted devices, not on local machines, unsecure servers, or unencrypted laptops or portable devices.
- provide appropriate physical security for information technology equipment, storage media, and physical data.
- make sure that confidential information is disposed of in a secure manner when it is no longer required.
- notify a Data Security Officer (www.bc.edu/datasecurityofficers) or the Director of Computer Policy and Security (security@bc.edu) upon becoming aware of any security breach or unauthorized access to confidential information, including Massachusetts PI.

In The News.....

Reducing Environmental Impact & Developing Sustainable Practices

Common Sense Tips to save energy and resources

- Shut down computers, turn off lights, printers and other electronics at the end of the day.
- Print double-sided; utilize the “Print Preview” option to avoid printing unnecessary pages.
- Take advantage of the University’s recycling: Keep a bin for recycling in your office space.
- Use reusable bottles and mugs to avoid daily waste from water/soda bottles or coffee/tea cups.