Columbia College Cyber Security Policy

Policy Brief & Purpose

This policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to the potential for severe security breaches. Human errors, hacker attacks, and system malfunctions could cause great financial damage and may jeopardize the College's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy:

Scope

This policy applies to all our employees, contractors/ adjunct faculty, volunteers, and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Course outlines and curriculum
- Future projects and directions for the College
- Unpublished financial information
- Data of students/partners/vendors
- Student lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect Personal and Company Devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet, and cell phone secure. They can do this if they:

- Keep all devices password protected.

Document Name: Columbia College Cyber Security Policy
Document Number: ADM-P380
Revision #1   NOTE: Revisions to this document can be made following procedures outlined in Document #ADM-P014 – Document Control Policy and Procedures
Revision Date: March 19, 2020
Approved by: Tom Snell
Page 1 of 4

- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Keep Emails Safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee is unsure that an email they received is safe, they can connect with our IT team.

Manage Passwords Properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to. When passwords have been shared, it should be changed by the owner immediately following the point that the purpose of the original sharing once that has been fulfilled.
- Change their passwords every two months.

Transfer Data Securely

Transferring data introduces security risk. Employees must:

Document Name: Columbia College Cyber Security Policy
Document Number: ADM-P380
Revision #1   NOTE: Revisions to this document can be made following procedures outlined in Document #ADM-P014 – Document Control Policy and Procedures
Revision Date: March 19, 2020
Approved by: Tom Snell
Page 2 of 4

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT team for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.

Our IT team needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to our IT team. Our IT team must investigate promptly, resolve the issue, and send a companywide alert when necessary.

Our IT team is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional Measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.

- Avoid using auto sign-in features for Columbia College log-ins, including any tool that would contain confidential Columbia College information.
- Report stolen or damaged equipment as soon as possible to their manager and the IT department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

- Avoid saving Columbia College confidential materials on personal devices

Our IT team should:

- Install firewalls, anti-malware software, and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Document Name: Columbia College Cyber Security Policy
Document Number: ADM-P380
Revision #1   NOTE: Revisions to this document can be made following procedures outlined in Document #ADM-P014 – Document Control Policy and Procedures
Revision Date: March 19, 2020
Approved by: Tom Snell
Page 3 of 4

Remote Employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standard and settings, and ensure their private network is secure.

We encourage them to seek advice from our IT team.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take Security Seriously

Everyone, from our students and partners to our employees and adjunct faculty, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Please refer to Columbia College Remote Access Policy for further information

Document Name: Columbia College Cyber Security Policy
Document Number: ADM-P380
Revision #1   NOTE: Revisions to this document can be made following procedures outlined in Document #ADM-P014 – Document Control Policy and Procedures
Revision Date: March 19, 2020
Approved by: Tom Snell
Page 4 of 4