Passwords and Security

What are the best practices for data security and privacy at Carthage?

Best Practices for Data Privacy and Security at Carthage College

Protecting Data from Unauthorized Access

Questions to answer:

- What data should be protected from unauthorized access? and why?
- How can I protect my data, the data of others, and the College's data from unauthorized access?
- What are the primary ways that data can be exposed, and how can I help prevent that?
- What laws and policies exist that regulate data access?
- What is your obligation as a Carthage employee related to data privacy?
- What are any possible consequences of data security breaches?

The law and data privacy:

- Wisconsin Act 138 concerns data privacy as related to potential for identity theft. See https://docs.legis.wisconsin.gov/2005/related/acts/138
- FERPA is the Family Education Rights and Privacy Act
- HIPAA relates to health information, especially medical records
- Copyright Law relates to intellectual property

What everyone should know:

1. Users shouldn't store sensitive information locally on computers that could be stolen
2. Users should protect access to both computers and systems with good password practices

3. Some internet-based storage and transmission methods are safer than others; learn the difference

TOP 10 SECURITY TIPS:

1. Don’t store data locally for others that would allow for identity theft (Act 138)
2. Don’t let your computer store passwords to any sensitive systems
3. Don’t use the same passwords for work and personal accounts and resources
4. Don’t use unsupported tools with your Carthage credentials (e.g. password storing sites, recreational sites, etc.)
5. ALWAYS check the validity of any request to login or provide your password
6. E-mail is inherently non-secure. Email communications go over the internet in plain text. Never provide sensitive data via email.
7. Make sure, when logging in anywhere, that the site address begins with https:// to know that the communication is encrypted.
8. If you ever believe that your account security has been compromised, change your password IMMEDIATELY for any and all accounts with that same password.
9. Physically secure your computer to protect it from theft
10. Don’t download or install additional software onto your work computer or any computer that has access to systems or data that should be kept confidential.

Unique solution ID: #1380
Author: smueller2
Last update: 2019-08-08 00:25