Data Privacy in an Era of **Compliance**

CYBER SECURITY JANUARY 2019

The internet is full of data about you. Whenever you play a game, shop, browse websites, or use any of numerous apps, your activity and some of your personal information may be collected and shared.

Similarly, the business of higher education requires us to collect, process, and store the digital information of others. Whenever we handle such information, we need to think about how we want our own information treated and treat other people's data with the same care and respect.

Protect yourself by following these tips:

- Know what you are sharing
  Check the privacy settings on all of your social media accounts; some even include a wizard to walk you through the settings. Always be cautious about what you post publicly..
- Guard your date of birth and telephone number
  These are key pieces of information used for identity and account verification, and you should not share them publicly. If an online service or site asks you to share this critical information, consider whether it is important enough to warrant it.
- Keep your work and personal presences separate
  Your employer has the right to access your email account, so you should use an outside service for private emails. This also helps you ensure uninterrupted access to your private email and other services if you switch employers.

Protect the information, identity, and privacy of others by following these tips:

- Know what resources are available at your institution
  Colleges and universities might employ individuals with some of the following titles and responsibilities: compliance officer, who can help you navigate the laws and regulations that govern how your institution handles constituents' personal data and what safeguards need to be implemented to ensure the data stay secure; data privacy officer, who can answer questions about how your institution protects the privacy of both your data and constituents' data; and a(n) (chief) information security officer, who can answer questions about information security best practices and the technologies available to protect online identity and the personal data of constituents.
- Know what policies are in place at your institution
  A privacy policy governs how the institution collects, processes, stores, and deletes the personal data of constituents; a data classification policy governs how the institution organizes the data it interacts with and what rules are in place for processing it; and an information security policy articulates how the institution governs and prioritizes information security activities.
- Confidentiality
  Keep constituents' personal information confidential and limit access to the data
- Only use data for its intended purpose
  If you need to use data for another reason, always check relevant resources and policies first for guidance.
- Destroy or De-identify
  Destroy or de-identify private information when you no longer need it.