# Higher Education Data Privacy & Cybersecurity Series

## Higher Education Policies & Procedures
## March 30, 2023

BOND SCHOENECK & KING ATTORNEYS

1

## Introductions

**E. Katherine Hajjar, Esq.**
Senior Counsel – New York, NY
Higher Education Practice
khajjar@bsk.com | (646) 253-2324
https://www.bsk.com/people/e-katherine-hajjar

**Shannon A. Knapp, Esq., CIPP/US**
Associate – Syracuse, NY
Cybersecurity and Data Privacy Practice
sknapp@bsk.com | (315) 218-8306
https://www.bsk.com/people/shannon-a-knapp

BOND SCHOENECK & KING ATTORNEYS

2

# Overview

- Why Data Privacy and Cybersecurity Are Important for Higher Education
- Website Policies and Procedures
- IT-Specific Policies
- Employee Facing Policies & Student Policies and Procedures
- Approaches to Policy Management

BOND SCHOENECK & KING ATTORNEYS

3

# Areas of Risk for Higher Education Institutions

- General Counsel's office records
- Admissions
- Financial Aid
- Student health records
- Student discipline records
- Registrar records (grades, transcripts)
- Institutional Research
- Human Resources
- Finance
- Research
  - Data
  - Grants and Contracts
- Alumni Records
- Study Abroad Programs
- Development
  - Donations/Donor lists
  - Research on donors (wealth estimates, planned giving details)
- Medical schools
- Hospitals—PII, insurance information, patient records
- Credit Unions
- Enrollment
- Marketing
- Board of Trustees/President
- Faculty
- Athletics
- IT

BOND SCHOENECK & KING ATTORNEYS

4

# Why Data Privacy & Cybersecurity Policies and Procedures Are Important for Higher Education

BOND SCHOENECK & KING ATTORNEYS

5

## Massive Amounts of Personal & Financial Data

- Student Identifying Information
- Personal Contact Information
- Personal Account Information
- Financial Details
- Health Care Information

BOND SCHOENECK & KING ATTORNEYS

6

## Other Reasons:

- Data Privacy Compliance
  - Global Array of Data Privacy Laws
  - Legal Obligations and Rights
- Cybersecurity Threats
  - Variety of cyber threats
  - Increased Attacks on Education/Research
    - In 2021: Increased 75% (1,605 attacks per HEI per week)
    - In 2022: Increased 44% (2,297 attacks per HEI per week)[1]
  - High Success Rate
    - In 2021: 74% of cyberattacks on colleges and universities were successful
      - *Compare with* 68% in business sector; 61% in healthcare; 57% in financial sector

BOND SCHOENECK & KING ATTORNEYS

7

# Website Policies & Compliance

BOND SCHOENECK & KING ATTORNEYS

8

## Privacy Policy

- A “privacy policy” is a document that describes a HEI’s general practices concerning the personal information that it obtains in the course of its operations. These policies help website visitors understand what is happening with their personal information.
- **Why are they important?**
  - Proliferation of privacy laws, as well as the indication by the Federal Trade Commission (FTC) and other enforcement agencies that it is best practice to include privacy policies and similar notices on websites.
  - Website user’s expectations regarding personal data privacy are rising in the wake of high-profile data breaches in both the for profit and nonprofit sectors.
  - A privacy policy is an important tool to build trust and transparency with your stakeholders, donors and other visitors to your website.
- Privacy policies should be customized for each HEI and site based on the specific data practices that are occurring

BOND SCHOENECK & KING ATTORNEYS

9

## Terms of Use

- A website "terms of use” (sometimes referred to as “terms of services” or “terms and conditions”) is intended to be a legally binding contract between a website’s owner and the website’s users.
- Establishing terms of use allows HEIs to outline rules and regulations for website visitors. It also provides protection for HEIs by limiting liability and providing recourse in case of misuse of the website or the information that it provides.
- Like a privacy policy, a terms of use needs to be customized for each HEI and site.

BOND SCHOENECK & KING ATTORNEYS

10

## Cookie Policy

- A "cookie policy" is a document that informs users of the types of cookies a website uses, how the cookies are used, and instructs users how to opt out or change the website's cookie settings.
  - **What is a "cookie"?**
    - A "cookie" is a small, encrypted file that websites store on your device that function as short-term memory for your browser. Cookies are generally used to personalize a user's web experience.
      - *For example,* cookies allow a website to remember items in a digital shopping cart or save a user's language preference.
- A cookie policy should include items such as:
  - (i) the types of cookies used, (ii) the personal data the cookies process, (iii) where the personal data will be transferred/processed, (iv) the purpose of the cookies, (v) how long the cookies will track the user, and (vi) how users can opt out of cookie usage.

BOND SCHOENECK & KING ATTORNEYS

11

## Cookie Notice/Pop-Up ("Cookie Banner")

- Under some international data privacy laws, websites and other applications must obtain a user's consent before using cookies.
- A website or application can satisfy the requirement by using a cookie notice/pop-up or a "cookie consent banner" that explicitly requests a user's consent to use cookies.
- A cookie notice/pop-up or banner must be:
  - (1) Sufficiently noticeable and in an easily accessible form;
  - (2) Written in clear, plain, and unambiguous language for the average user; and
  - (3) Provide enough information for a user to make an informed choice;
  - (4) Provide a clear action whereby users can consent or refuse to consent.

BOND SCHOENECK & KING ATTORNEYS

12

## Cookie Compliance

- **EU's ePrivacy Directive & General Data Protection Regulation ("GDPR"):**
  - Require explicit and informed consent prior to use of all non-exempt cookies.
  - **Who must comply?**
    - Any website operating in the EU and any website outside the EU that collects data from users inside the EU.
  - **Application to US Higher Education Institutions**:
    - Even if the institution has no establishment in the European Union, if the institution collects or uses personal data from individuals in the EU, GDPR applies.
      - *Example*: Student recruitment – universities that collect personal data when recruiting students located in the EU will have to comply with GDPR requirements.
  - May become more necessary as new technology is adopted on websites beyond just cookies. Example: Session Replay Technology

BOND SCHOENECK & KING ATTORNEYS

13

## IT-Specific Policies

BOND SCHOENECK & KING ATTORNEYS

14

## IT-Specific Policies

- Business Continuity and Disaster Recovery Plan
- Asset Management Policy
- Encryption Management Policy
- Identity and Access Management Control Policy
- Network Management Policy
- Risk Management Policy
- Security Training and Awareness Policy
- System Development and Acceptance Policy
- Vulnerability Management Policy
- Incident Response Plan

BOND SCHOENECK & KING ATTORNEYS

15

## Business Continuity & Disaster Recovery Plan

- A "business continuity and disaster recovery plan" is a set of strategies, policies and procedures that help a HEI respond to and continue its operations during a data emergency and recover to full operations following the emergency.
- Its role is to minimize the effects of outrages or other disruptions on business operations that may occur.
- Business Continuity v. Disaster Recovery:
  - Business Continuity is more proactive and generally refers to processes and procedures that must be in place to ensure critical functions continue to run.
  - Disaster Recovery is more reactive and outlines specific steps required to resume operations after an incident.
- A BCDR plan should have policies and procedures to address events that could hinder business continuity.
  - Such events may include – cyberattacks and data breaches, power outages, climate change/natural disasters, or infrastructure failure.

BOND SCHOENECK & KING ATTORNEYS

16

# Incident Response Plan ("IRP")

- An "incident response plan" is a document that instructs IT and cybersecurity professionals on how to respond to a serious security incident (e.g., data breach, data leak, ransomware attack, or loss of sensitive information).
- Four Phases of an effective IRP:
  - (1) Preparation
  - (2) Detection and Analysis
  - (3) Containment, Eradication, and Recovery; and
  - (4) Post-Incident Activity
- **Why is an IRP important?**
  - An IRP enables a HEI to detect and respond to cyberattacks more quickly, minimizing the duration and damage of security incidents.
    - In 2022:
      - Average time to identify and contain a data breach – 277 days
      - Average cost of a data breach – $4.35 million

BOND SCHOENECK & KING ATTORNEYS

17

# Risk Management Policy

- A "risk management policy" sets out the HEI's processes and procedures to identify and respond to risks specific to the HEI and minimize their impact.
- HEIs must manage information security risks on an ongoing basis.
- Can encompass vulnerabilities and cyber risks, as well as how the institution's devices, networks, and assets are protected and managed.
- Policy should assign authority to create, oversee, and enforce processes, such as:
  - (i) Risk assessment,
  - (ii) Risk mitigation and remediation,
  - (iii) Vulnerability management, and
  - (iv) Compliance Management

BOND SCHOENECK & KING ATTORNEYS

18

## Risk Assessment

- "Risk assessment" allows a HEI to identify reasonably foreseeable internal and external risks and to assess the sufficiency of safeguards to control the identified risks.
- A HEI must periodically perform risk assessments regarding the sufficiency of the institution's existing safeguards.
- **What to look for:** potential threats, vulnerabilities (including administrative, technical and physical), probability of harm, harm that is likely to result from particular events.
- **Potential risks in Higher Education:**
  - Phishing, Ransomware, and other cyberattacks
  - Inadequate security tools
  - New vulnerabilities regarding Post-COVID-19 digital campus

BOND SCHOENECK & KING ATTORNEYS

19

# Employee Facing Policies & Student Policies and Procedures

BOND SCHOENECK & KING ATTORNEYS

20

## Employee Facing Policies & Student Policies

- Information Governance Policy
- Information Security Policy
- Acceptable Use Policy
- Bring Your Own Device Policy
- Information Classification and Management Policy
- Electronic Workplace Monitoring and Surveillance
- Remote Access Policy
- Electronic Monitoring Policy (NYS, DE and CT)
- Protecting Personal Identifying Information Policy
- Breach Notification Policy
- Incident Response Policy
- Vendor Management Policy
- Records Management and Destruction Policy
- Social Media and Social Networking Policy

BOND SCHOENECK & KING ATTORNEYS

21

## Information Security Policy

- Establishes information security as core value of HEI
- Lays out clear rules and standards for using and protecting information assets
- Helps workforce members understand risks
- Provides a basis for training and ongoing awareness
- Should apply to all workforce members, including employees, contractors, volunteers, student workers, and any others accessing or using the institution's information assets.
- Policy v. Plan: A policy is accessible to the entire workforce, whereas a robust information security plan applies the policies, adopts to changing risks, and is usually owned or adopted by specific groups (ex. IT)

BOND SCHOENECK & KING ATTORNEYS

22

## Acceptable Use Policy

- Document that outlines the constraints and practices that employees, students, etc. must agree to in order to use the institution's network, internet, and other information assets
- Management of faculty, staff, and student use of HEI devices, networks, and listserv
- Should be signed/agreed to during the onboarding or orientation process
- Example clauses: use in compliance with applicable law, do not hack the network, do not send spam/mass emails, report any suspicious activity, etc.

BOND SCHOENECK & KING ATTORNEYS

23

## Bring Your Own Device Policy

- Expectations
  - Data ownership, no expectation of privacy, register device, permit access to employer, consequences for noncompliance, cost and reimbursement
- Security Precautions
  - Reporting requirements, security software, strong passwords, configuration requirements, international travel
- Appropriate Use
  - Device not used for harassment/discrimination, work hours for nonexempt employees, end of employment

BOND SCHOENECK & KING ATTORNEYS

24

## Data Retention & Destruction Policy

- A "data retention and destruction policy" is a HEI's protocol for maintaining and destroying information. A HEI can ensure that it complies with local, state, federal and international laws and regulations by setting a proper data retention period.
- A data retention policy can make data cleaner and more accessible while reducing costs associated with data storage and e-discovery.
- **Application to US Higher Education Institutions**:
  - Data retention policy must comply with applicable state and federal laws and regulations, including the DOE, HIPAA, FLSA, FERPA, among others.
  - Relevant particularly for admissions and alumni relations

BOND SCHOENECK & KING ATTORNEYS

25

## Vendor Management Policy

- Identifies vendors used by institutions, prioritizes them, and identifies the risks associated with each vendor
- Assigns roles in vendor management process
- Defines the controls required to minimize risks associated with vendor
  - Ex. required contractual provisions, required certifications, etc.
- Outlines required assessment/due diligence process
  - Evaluate vendor's policies, procedures, insurance, and training materials on data privacy and cybersecurity

26

BOND SCHOENECK & KING ATTORNEYS

## Compliance Policies for Applicable Laws

- Certain laws that HEIs may be subject to require specific policies for compliance
- GDPR Examples:
  - Legal Basis Chart: Outlines the legal basis relied upon by the institution for processing of all data covered by GDPR.
  - Data Subject Access Request (DSAR)/Data Subject Request Policy: Policies that outline how the institution will respond to and fulfill data subject requests.
  - Data Processing Agreement: Document used to regulate data protection with vendors that sets out GDPR and other minimum data protection and cybersecurity requirements.

BOND SCHOENECK & KING ATTORNEYS

27

## Approaches to Policy Management

- Coordination of various offices and departments that "own" these policies
- Run exercises (ex. tabletop exercises) with response teams on hypothetical breaches
- Routine review -- these should be "living" documents and should be updated and reviewed regularly

BOND SCHOENECK & KING ATTORNEYS

28

# Upcoming in the Series:

**Part Four:** **Higher Education Cybersecurity & Data Breach Response** (April 13, 2023)
By: Jessica Copeland, Seth Gilbertson

**Part Five:** **Data Privacy & Higher Education Marketing & Admissions** (April 27, 2023)
By: Mario Ayoub, Amber Lawyer, Jane Sovern

**Part Six:** **Cybersecurity Insurance** (May 11, 2023)
By: Gail Norris, Gabe Oberfield

BOND SCHOENECK & KING ATTORNEYS

29

# Questions?

**E. Katherine Hajjar, Esq.**
Senior Counsel – New York, NY
Higher Education Practice
khajjar@bsk.com | (646) 253-2324
https://www.bsk.com/people/e-katherine-hajjar

**Shannon A. Knapp, Esq., CIPP/US**
Associate – Syracuse, NY
Cybersecurity and Data Privacy Practice
sknapp@bsk.com | (315) 218-8306
https://www.bsk.com/people/shannon-a-knapp

BOND SCHOENECK & KING ATTORNEYS

30

# Thank You

The information in this presentation is intended as general background information.
It is not to be considered as legal advice.
Laws can change often, and information may become outdated.



BOND SCHOENECK & KING ATTORNEYS