FISHER COLLEGE

Data Privacy, Security and Identity Theft Committee

Incident Response Plan

The Fisher College Data Privacy, Security and Identity Theft (PSIT) Committee Incident Response Plan[1] is intended to provide direction and guidance….

❖ Policy

Users of electronic resources[2] connected to the Fisher College network, as well as all users of College data, must promptly report all suspected and actual data, cyber security, and/or identity theft incidents. Fisher College's PSIT Committee is responsible for evaluating incidents for a breach of College data, including Personal Identifiable Information (PII) held by the College, and when necessary to initiate this Incident Response Plan.

Reason for Policy

Prompt and consistent reporting of Cyber Security Incidents[3] protects and preserves electronic resources and institutional data and aids the College's compliance with applicable law.

Scope

This policy applies to electronic resources, regardless of ownership or location, used to store, process, transmit or access College Data, as well as all Users of College Data[4].

❖ Responsibilities of Users

Users are required to immediately report suspected or actual Cyber Security Incidents to Fisher College Data Privacy, Security and Identity Theft (PSIT) Committee at PSIT@fisher.edu and/or Fisher College Information Services at is-team@fisher.edu or 617-236-8852. Examples include but are not limited to:

- Confirmed or suspected malware impacting electronic resources or with the potential to infect College data
- Malicious email targeting College data
- College data discovered to have been unsecured or accessible by unauthorized parties
- Theft of College-owned property
- Impairment of Fisher's electronic resources

[1] See Definitions, page 5
[2] See Definitions, page 5
[3] See Definitions, page 6
[4] See Definitions, page 6

Users are required to follow the instructions provided by Fisher College PSIT Committee after reporting an incident, and to cooperate in any investigation of the incident by the College.

To the extent that the incident is occurring with a user's assigned electronic resources, if directed by Fisher College PSIT Committee, the user will cease use of the actual or suspected resource immediately, understanding that continued use may inadvertently damage potential evidence if the incident becomes part of a criminal case or insurance claim.

Users who encounter a suspected or actual incident are required to take all possible measures to preserve evidence, as directed by Fisher College PSIT Committee. For instance, if a user suspects their device has been compromised, they may be directed to power off the machine and deliver it unchanged to the IT Help Desk for investigation.

Users will not refer to a Cyber Security Incident as a "breach" unless they have been approved to do so by the Fisher College PSIT Committee.

Incident Notification

- All departments, units, and offices must include provisions in any third-party contracts requiring that the third party and third-party subcontractors provide immediate notification to the College of incidents involving College data or electronic resources and to report findings of investigations of such incidents.

- The College will investigate incident reports and will comply with any legal obligations to notify affected individuals and/or Federal, State entities.

- Notification may be delayed in cases where law enforcement determines and advises that notice would impede an ongoing investigation.

❖ Compliance with this Policy

The Fisher College PSIT Committee shall ensure compliance with this policy and will ensure regular reviews, updates, and distribution of this policy. Violations of this policy may result in disciplinary action, in accordance with Fisher College's Human Resources and/or the Dean of Students Code of Conduct policies and any additional collective bargaining agreements.

❖ **Fisher College Incident Response Plan**

If a vetted incident is detected and the Fisher College PSIT Committee is alerted, the following procedure of the incident response plan will be activated:

The goal of this analysis is to examine data and discover all, or part of, an attack chain. Key events to document include:

• who or what originated the incident,

• what networks, systems, and applications are affected,

• how the incident is occurring (what tools or attack methods are being used and what vulnerabilities are being exploited),

• which users are logged onto the network,

• which systems and processes are running,

• current external connections to the computer systems, and

• all open ports and their associated services and applications.

Containment

To prevent further damage and to remove an intruder's access and control of systems, containment strategies will be implemented. Such containment activities may include, but are not limited to:

• isolate impacted systems and network segments;

• block (and log) unauthorized accesses and malware sources;

• close specific ports and mail servers, or other relevant servers and services; and

• reset system login credentials and revoke privileged access, if applicable.

Reporting

Per Title IV regulations, in accordance with Federal Student Aid (FSA), and in compliance with the GLBA Safeguards Rule under 16 C.F.R. Part 314, all vetted breaches will be reported to FSA by filling out the Cybersecurity Breach Intake Form found at https://fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity.

The following elements are reported within the FSA Cybersecurity Breach Intake Form:

- Breach Date
- Impact of Breach
- Method of Breach
- School Contact Information

- Remediation Status
- Details
- Next Steps

Once the Intake Form is completed, a member of the FSA Cyber Incident Team is assigned and may request follow up items. Recommendations for case closure or further steps may result.

In accordance with Massachusetts State law:

> "The Data Breach Notification Law requires businesses and others that own or license personal information of residents of Massachusetts to notify the Office of Consumer Affairs and Business Regulation and the Office of Attorney General when they know or have reason to know of a breach of security"

As such, all personal information, (as defined below) must notify both the Office of Consumer Affairs and Business Regulation and the Attorney General's Office of the breach. The notification must include:

- A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information;
- The number of Massachusetts residents affected as of the time of notification;
- The steps already taken relative to the incident;
- Any steps intended to be taken relative to the incident subsequent to notification; and
- Information regarding whether law enforcement is engaged investigating the incident.

Personal Identifiable Information (PII) is defined as,

(a) Social Security number;

(b) driver's license number or state-issued identification card number; or

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

PII does not include information that can be legally obtained from publicly available sources, such as addresses or birthdays.

Post-Incident Analysis

After concluding cyber incident recovery activities, the Fisher College PSIT Committee conducts a post-incident analysis to review the effectiveness and efficiency of this Plan including, but not limited to,

• incident root cause and mitigation efforts;

• infrastructure vulnerabilities and efforts to address;

• technical or operational training needs; and

• tools required to perform protection, detection, analysis, or response actions.

❖ **Definitions**

For purposes of this policy, the following definitions apply:

Incident Response Plan: Internal protocol for a team(s) of College staff responsible for response to cyber security incidents.

Cyber Security Events, Incidents, and/or Breaches:

1. Event — An exception to the normal operation of IT services, such as outages. Not all events are incidents or breaches.

2. Incident — Electronic activities that result in unauthorized access or exposure to College Data, or significant impairment of College IT systems. All incidents start as events.

3. Breach — The unauthorized acquisition or unauthorized use of either (a) unencrypted data or (b) encrypted electronic data along with the confidential process or key, that is capable of compromising the security, confidentiality, or integrity of personal information that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth. A good faith but unauthorized acquisition of personal information by Fisher College or its employees or agents for the lawful purposes of Fisher College is not a breach unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure. The term "breach" does not include disclosure of personal information when the disclosure is required by court order or necessary to comply with state or federal regulations.

Data Breach Notification: The College's notification requirements in response to a Cyber Security Incident.

Electronic Resources: Any electronic asset (including devices and data) owned or handled by Fisher College.

Encryption: Security method that renders data elements unreadable by unauthorized parties.

The Information Security Officer (ISO) is the IT professional responsible for:

- Ensuring the prompt investigation of an incident
- Ensuring the preservation of evidence relating to an incident
- Determining what College data may have been exposed
- Securing any compromised systems to prevent further damage
- Providing guidance to institutional stakeholders
- Developing and distributing an after-action analysis
- Working with external law enforcement when necessary

Personal Information:

> Per the Massachusetts regulation for Personal Information and Breach of Security, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security Number; (b) driver's license number or state-issued identification card number; or (c)
>
> financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number ("PIN"), or password that would permit access to a resident's financial account. The term "personal information" does not include that information which is lawfully obtained from publicly available information (such as addresses or birthdays), or from federal, state, or local government records lawfully made available to the general public.

Regulated Data: Data that requires the College to implement specific privacy and security safeguards as mandated by federal, state, and/or local law, or College policy or agreement.

Users of College Data: Any person extended access and use privileges to College data. Includes students, faculty, visiting faculty, staff, volunteers, alumni, persons hired or retained to perform work for the College, and any other person extended access and use privileges by the College under contractual agreements or otherwise.