Cybersecurity Policy for Illinois Tech

Drafted by:

1. Michal Markevych
2. Neha Dalpe
3. Pavan Sadarshan
4. Griselda Pasillas
5. Thomas Carmody

1.0 Overview

Illinois Institute of Technology is currently a private institution focusing on STEM education for both undergraduate and graduate students. While attempting to provide a quality education, it aims to provide a manageable security system to help protect private data. IIT has the responsibility to protect student information and data that is being stored by all departments. In doing so, IIT hopes to play a role in its student development, gain recognition as being a Premier Technology Focused University, become a leading University, and improve financial support. This policy will discuss in detail the vulnerabilities IIT's website has and will address new security measures that need to be applied to further prevent any cyber attacks.

2.0 Purpose

Implementing an effective information security policy relies heavily on 3 important principles that the university would like to follow: confidentiality, integrity and availability ("What are", n.d) . We want staff members and students to feel safe using university resources. Confidentiality focuses on allowing the appropriate access to certain users. Students would have certain capabilities and restrictions while staff members would have administrative access with little to no restrictions. Integrity would focus on validating that all information is accurate and is only modified by authorized users, and availability will push for authorized users to be able to access the system when it is down to help control any technical interruptions. This is crucial as IIT's website domain is operated by each department, research groups and more. The policy outlined below was orchestrated by our security team and will discuss in detail what changes need to be made to achieve all the university's goals by highlighting vulnerabilities in authentication, and bringing to light mishandled internal errors. Another purpose of this policy is to outline how Federal controlled information will be treated. This policy addresses some of the existing weaknesses of SSL certificates and configurations, web application headers, and cross-site scripting.

3.0 Scope

This policy applies to all users accessing the iit.edu domain. This also includes anyone using IIT's information technology resources including visitors, students, staff, faculty, research parties, and other parties with access to IIT data.

4.0 Policy

4.1 Web pages should have security tests conducted regularly based on the following:

- New/Major Release; Will be liable to a full test before the clearance of the change control documentation and/or the liberation into the live environment.
- Enhancement Releases; Will be liable to the proper testing level based on the risk of the adjustments made to the functionality of the application/architecture.
- Patch Releases; Same as Enhancement Releases.
- Emergency Releases; A release of an urgent nature will be given permission to relinquish security tests and hold on to the risk until enough time for the test to complete has passed. These types of releases are to be designated by the proper manager or Chief Information Officer (CIO).

4.2 The risk levels listed below are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- Critical: Critical issues allow an adversary to readily gain control of the target system and potentially compromise other systems or networks. Vulnerabilities may provide an attacker with full read and/or write access to sensitive data, remote execution of commands, and the ability to deploy malware. Illinois Tech recommends that all Critical issues be remediated immediately.

- High: High-risk issues are those most likely to cause disruption of service, disclosure of unauthorized information, or other significant negative consequences. Only issues with a High impact and Medium or High exploitability rating are considered to be High risk. Illinois Tech recommends that all High-risk issues be remediated.

- Medium: Relative to High-risk issues, Medium risk issues have less significant impacts or are more difficult to exploit. Attacks that can only be executed by limited subsets of users, or that do not lead directly to a system or account compromise, are frequently ranked as Medium risk issues. Illinois Tech recommends that all Medium risk issues be remediated.

- Low: Low-risk issues have limited impact (e.g., disclosure of non-sensitive information) or can only be executed by a very limited set of trusted users (e.g., an attack that could only be carried out by an administrator). Although Low-risk issues should still be considered threats to the organization's security posture, the organization may choose to accept the risk from these issues rather than address them. In most cases, Illinois Tech recommends addressing these issues.

4.3 Acceptable Use Policy (AUP)

An AUP stipulates the constraints and parties that an employee in Illinois Tech using organizations assets must agree to in order to access the organization network or the internet. It is a standard onboarding policy for employees. It is recommended that IT, security, legal and HR departments discuss what is included in this policy.

4.4 Information Security Policy

A robust security foundation is crucial to protect the University's information and IT assets. It is the policy of Illinois Tech to manage nonpublic personal financial information collected from customers as confidential records. Illinois Tech has developed and will continue to develop appropriate procedures to protect such financial information against reasonable threats and hazards and unauthorized access or use of such records that could result in substantial harm or inconveniences to their customers. As the iit.edu website is operated at many levels, transparent flow of information and changes shall be established. The relations between IT and security staff in different departments play a crucial role.

4.5 Sensitive data risk

The university manages various types of sensitive information and Personally Identifiable Information (PII), payment details, research data, student records, data subject to compliance. To safeguard this information, a thorough understanding of the nature of information, where to store, how it is created, transmitted, shared, stored, and deleted is critical. This life cycle of data storage is vital.

5.0 Web Page Responsibilities

The Office of Technology Services (OTS) and the Center for Law and Computers (CLC) have devised specific rules and procedures applicable to Illinois Tech related web pages. All web pages contained with the iit.edu domains or served on IP addresses owned by Illinois Tech are subject to the following content guidelines, as well as other applicable Illinois Tech policies.

1. The content of the first-level pages on the Illinois Tech web site, https://www.iit.edu/ is designed and specified by the Office of Communications and Marketing

2. All other web pages contained within, except for individual faculty, staff and student pages, should follow the design standards set forth by the Office of Communications and Marketing and the Office of Public Affairs, as applicable.

3. All web pages should be secured using Transport Layer Security (TLS) and not SSL. All versions of TLS 1.0 and 1.1 are deprecated by Internet Engineering Task Force (IETF) as of March 25, 2021. Transition plans to TLS 1.2 or 1.3. It is recommended using TLS 1.3, as it is faster and more secure. Make sure the web servers support the latest versions.

4. All pages must clearly display at the bottom of the page the name and email address of the person responsible for the page.

5. Pages cannot contain or transmit any information that is illegal, pornographic, defamatory, obscene or harassing.

6. Users are prohibited from serving pages that conduct electronic commerce or contain paid advertising. Pages must not cause interference with the ability of other users to access network resources.

7. Pages that do not meet acceptable use or content standards are subject to immediate removal, and Users are subject to the suspension of web privileges as well as further disciplinary procedures as appropriate.

8. Student organizations and private, individual pages should link to a disclaimer stating that the content does not express the views of IIT.

9. Vulnerability testing on the webpages and server-side software must be performed and any affected software must be updated to the latest versions in order to eliminate any vulnerability.

6.0 Compliance Procedures

1. Each department is responsible for implanting and reviewing the practices to assure the procedures and steps taken by the teams/individuals are compliant with this policy. The Chief Information Officer (CIO) is responsible for enforcing this policy and is authorized to set specific password creation and management standards for university systems and accounts.

2. Inappropriate uses of Illinois Tech Resources should be reported to the Office of Technology Services via abuse@iit.edu. Security related questions and issues should be directed to security@iit.edu.

3. Any individual making inappropriate use of Illinois Tech resources and hindering from normal operations or acting in a manner contrary to the policy will be contacted and appropriate actions will be taken.

4. Any report or discovery of such action on Technology resource by any user may be denied access to Illinois Tech resources immediately without any warning and the alleged violation information will be provided to the appropriate Illinois Tech official who may then take action in accordance with the applicable policy.

5. Any report of data mishandling by a user can expect to see themselves phasing criminal sanctions or termination (subject to management's discretion).

7.0 Definitions

CIO: Chief Information Officer is the information technology director and highest executive in charge of reviewing policies and making sure they are correctly implemented.

CUI: Controlled Unclassified Information pertains to information created by or owned by the government that must be kept secure and have measures for dissemination(spreading) controls. This information is not classified nor business intellectual property but is important for national security.

OWASP: Open Web Application Security Project

References

Brathwaite, S. (n.d, December 23). *What are the 3 principles of information security?* Security Made Simple. Retrieved April 23, 2022, from https://www.securitymadesimple.org/cybersecurity-blog/what-are-the-3-principles-of-information-security

Cal Poly. (n.d.). *Cal Poly Information Security Program (ISP)*. Information Security. Retrieved April 23, 2022, from https://security.calpoly.edu/cal-poly-information-security-program-isp

"Introduction." *OWASP Top 10:2021*, https://owasp.org/Top10/.

National Cyber Command Centre. (n.d.). *Home*. NC4. Retrieved April 24, 2022, from https://nc3.go.ke/the-cia-triad/

"Owasp Web Security Testing Guide." *OWASP Web Security Testing Guide | OWASP Foundation*, https://owasp.org/www-project-web-security-testing-guide/.

Procedure Q3 Use of Technology Resources. Policies and Procedures Handbook Illinois Institute of Technology. (19AD). Retrieved April 24, 2022, from https://web.iit.edu/sites/web/files/departments/general-counsel/policies/procedure_q3_use_of_technology_resources.pdf

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021, January 28). *Protecting controlled unclassified information in nonfederal systems and organizations*. CSRC. Retrieved April 23, 2022, from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Security Policies. EDUCAUSE. (n.d.). Retrieved April 23, 2022, from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies