DATA SECURITY AND PRIVACY FRAMEWORK: TAU SIGMA NATIONAL COLLEGIATE HONOR SOCIETY'S INDUCTION MANAGEMENT SYSTEM

Abstract

This document presents a comprehensive overview of the data security and privacy measures implemented by Tau Sigma National Collegiate Honor Society in its Induction Management System (IMS). It details our commitment to safeguarding the personal data of potential inductees, specifically their names and email addresses, while aligning with the Family Educational Rights and Privacy Act (FERPA) regulations. Key areas covered include our approach to data encryption, server security, use of cookies, third-party collaborations, and FERPA compliance. The document underscores Tau Sigma's dedication to maintaining a balanced, effective, and transparent data security framework, ensuring the trust and confidence of educational institutions and students alike.

Randy Bowman

Principal Consultant, i5 Technology, LLC

CONTENTS

EXECUTIVE SUMMARY

At the Tau Sigma National Collegiate Honor Society (Tau Sigma), we implement a robust and sensible approach to data security within our Induction Management System (IMS), with a focus on effectively safeguarding student data. This document details our measured yet comprehensive strategy for data protection, aligned with the specific needs of our application and the types of data we handle.

Key highlights of our data security approach include:

- **Targeted Encryption and Security Measures:** We employ strong encryption and security protocols tailored to the nature of our data. These measures are designed to provide effective protection without imposing unnecessary complexity.

- **Adherence to FERPA Guidelines:** Our practices are in strict compliance with the Family Educational Rights and Privacy Act (FERPA), ensuring responsible handling and privacy of student data.

- **Selective Third-Party Collaboration:** We engage with third-party service providers, such as i5 Technology LLC, Hostek, and Twilo SendGrid, only after thorough vetting to confirm their alignment with our data security standards.

- **Regular Review and Adaptation:** Our data security protocols are regularly reviewed and updated, reflecting our commitment to maintaining a secure and responsive data environment.

- **Open Communication Policy:** We maintain transparency and are always available to address any inquiries or concerns about our data security practices, fostering trust and clarity with our clients.

This overview conveys our dedication to maintaining a secure data environment, balancing effectiveness with practicality, and ensuring the trust of the educational institutions we partner with.

DATA COLLECTED

Tau Sigma collects limited personal data, specifically first name, last name, and email addresses, of transfer college students who meet our eligibility criteria for induction. These data elements are considered low risk with respect to privacy and security concerns. This is because they do not include sensitive personal information (such as Social Security numbers, financial data, or health records) that could lead to significant harm or identity theft if compromised. Our focused collection approach aligns with best practices for data minimization, further reducing potential risks associated with data privacy and security.

DATA USAGE

Tau Sigma responsibly utilizes the collected data - first name, last name, and email addresses - for the sole purpose of extending invitations to eligible students to join the honor society. Each student receives a maximum of three emails: an initial invitation followed by up to two reminders. These reminders are only sent to those who haven't responded, ensuring respectful communication frequency.

To uphold our commitment to data privacy and individual choice, each email features a straightforward “unsubscribe” link. This link enables prospective inductees to opt out of further communication instantly, without any hindrances or delay. Our unsubscribe process is designed to be user-friendly and respects the recipient's decision unequivocally.

Upon acceptance of the invitation, the student enters into a direct relationship with Tau Sigma. From this point onwards, the management of the member's data privacy falls under the purview of Tau Sigma and is regulated by our own privacy policies, distinct from university oversight.

After the conclusion of the induction period, we retain the basic information of invitees solely to prevent any future re-invitation, as Tau Sigma offers a one-time invitation only. This retention is aligned with our data minimization strategy, ensuring that the data is used only for this specific and necessary purpose, further mitigating privacy risks.

SECURITY MEASURES

1. **Data Encryption in Transit:** Our IMS employs a 256-bit encrypted SSL certificate, a high standard in data encryption. This means any data transferred between the user's device and our system over the public internet is encrypted, significantly reducing the risk of interception by unauthorized parties.

2. **Hosting and Firewall Protection:** The IMS is hosted on a Virtual Private Server (VPS), which offers a secure and isolated environment for our operations. The server is fortified with firewall protection, acting as a barrier against cyber threats. We meticulously manage network access, keeping most ports closed or restricted. Specifically, only essential ports such as 21 (FTP), 990 (SFTP), 80 (HTTP), and 443 (HTTPS) are open, minimizing potential vulnerabilities.

3. **Use of Session Cookies:** To enhance the user experience during the invitation acceptance process, our IMS uses temporary session cookies. These cookies are essential for maintaining the session's continuity and are securely managed. Importantly, they are automatically destroyed once the invitee ends their web browsing session, ensuring no residual data is left on the user’s device.

4. **No Persistent Cookies:** Our system is designed to function efficiently without the need for persistent cookies. This means we do not store any long-term cookies on the user's device, which aligns with our commitment to privacy and minimal data footprint.

THIRD-PARTY PARTNERSHIPS AND DATA SECURITY

Tau Sigma maintains strict control over inductee information, sharing it with external companies only under specific, secure conditions. Our partnerships are governed by stringent agreements to ensure the protection and confidentiality of inductee data.

1. **i5 Technology LLC - Software Development Services:**
    - **Role:** i5 Technology LLC assists Tau Sigma with software development consulting services, which may involve access to inductee information.
    - **Data Security Agreement:** A robust confidentiality clause within our agreement strictly prohibits i5 Technology LLC from sharing, disclosing, or using inductee data for any purpose other than providing direct services and support to Tau Sigma.
2. **Hostek - Cloud-based Hosting Services:**
    - **Role:** Hostek provides the hosting services for the IMS.
    - **Security Measures:** In addition to a contractual prohibition against accessing or using client data, Hostek fortifies our data with multiple layers of security:
        - Advanced server protection with ESET Server Security or Avast Server Security.
        - Regular updates for operating systems and ColdFusion.
        - Dedicated firewalls for each server.
        - Network Intrusion Prevention services.
    - **Certifications:** Hostek is both SOC-2 Certified and PCI-Compliant, ensuring adherence to high standards of security and data handling.
3. **Twilo SendGrid - Bulk Email Services:**
    - **Role:** Twilo SendGrid manages bulk email dispatch for Tau Sigma.
    - **Data Privacy Commitment:** They do not sell or misuse recipient email addresses.
    - **Data Center Security:** All SendGrid data centers are SOC-2 Certified, ensuring a high level of security.
    - **Data Encryption:** All data transferred from the IMS to SendGrid is encrypted during transit, safeguarding it against unauthorized access.

Each third-party service provider is rigorously vetted by Tau Sigma to ensure their practices align with, or surpass, our own standards for securing student data. This careful selection process reflects our unwavering commitment to maintaining the highest level of data security and privacy.

COMPLIANCE WITH FERPA

Tau Sigma's data collection and handling practices are designed with a keen awareness of, and adherence to, the Family Educational Rights and Privacy Act (FERPA) regulations. While recognizing that institutions may have their own more restrictive policies, our approach to data collection is in line with the general understanding of FERPA's provisions.

Nature of Data Collected:

- The data points collected by Tau Sigma — first name, last name, and email addresses of potential inductees — are typically classified as "directory information" under FERPA.

- Such information is generally not considered harmful or an invasion of privacy when disclosed. This classification is crucial as FERPA allows for the release of directory information without prior consent from the student, provided the student has not opted out of such disclosure.

Tau Sigma's Compliance Measures:

- **Data Use Limitation:** The use of collected data is strictly confined to the purposes of inviting eligible students to join the honor society, in line with the permissible uses under FERPA.

- **Data Security and Privacy:** Even though the collected data falls under the less restrictive category of directory information, Tau Sigma applies appropriate data security and privacy measures to ensure its protection, reflecting our commitment to respecting student privacy beyond the requirements of FERPA.

Ongoing Review and Adaptation:

- Tau Sigma continuously reviews its data handling practices to ensure alignment with any changes or updates in FERPA regulations, demonstrating our ongoing commitment to compliance and the protection of student privacy.