Information Security and Technology Use Policy

[Your Organization's Name Here] is committed to respecting the privacy of our *[clients/customers/volunteers]* and to protecting Personally Identifiable Information from unauthorized access. To that end, the following policy for information security and technology use has been established.

Attendee Personally Identifiable Information (PII) – PII refers to information that, when used alone or combined with other information, can be used to identify a specific individual. This information includes but is not limited to name, mailing address, email address, telephone number, date of birth, passport number, etc.

[Your Organization's Name Here] employees *[and volunteers?]* are responsible for ensuring:

- Attendee PII is handled in a manner that honors *[Your Organization's Name Here]*'s desire to protect information from any outside party.

- Attendee PII is not disclosed to any outside party without approval from the *[Your Organization's Name Here]* Director of Operations.

- No website or system captures PII without approval from the *[Your Organization's Name Here]*'s Director of Operations. *This includes asking attendees to create an account in order to access a website or system.*

- Attendee PII is not exported and stored in systems or tools outside of those necessary to fulfill work responsibilities. *For example, when data is exported into Excel, employees are responsible for ensuring it is secure and not accessible to any outside party.*

- Computer and tablet screens are locked when unattended.

- Work space (on-site and off-site) is left clear of attendee PII.

- Personal use of computers, tablets, software, and telecommunication systems does not interfere with the ability to protect attendee PII.

Credit Card Information

[Your Organization's Name Here] employees are responsible for ensuring:

- No credit card information is collected except through approved systems. *If you have questions about approved systems, contact the Technology Services Support Manager.*

- No credit card information is stored in ***any way***. It is ***strictly prohibited*** to store:

1. Credit card numbers.
2. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
3. The CVV/CVC (the three- or four-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
4. The PIN or the encrypted PIN Block under any circumstance.

Technology Use (computers, tablets, software, applications, networks, websites, etc.)

[Your Organization's Name Here] employees are responsible for ensuring:

- Accounts and passwords for any computer, tablet, software, database, or network device (including those belonging to an approved third party) are kept secure and are not shared.

- Computer and tablet screens are locked when unattended.

- Computers and tablets are kept secure when not on-site. *For example, don't leave a computer or computer bag in plain sight in your vehicle.*

- No connection or access to a computer, tablet, database, website, or network device is given to a third party without approval from the *[Your Organization's Name Here]* Infrastructure Manager.

- No hardware, software, or network device is installed without approval from the *[Your Organization's Name Here]* Infrastructure Manager.

- No computer, tablet, or software setting is manipulated to circumvent security measures. *This includes changing computer network DNS settings, creating VPN tunnels, misusing computer administrator accounts, renaming devices, removing antivirus software, etc.*

- Email, internet, computers, tablets, and other *[Your Organization's Name Here]* resources are not used to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal.

Information security incidents, including the theft of a computer or the unauthorized access of a website or database, must be reported immediately to the Technology Services Support Manager.

As employees, we each have a responsibility to ensure *[Your Organization's Name Here]* clients' information and technology systems are protected from unauthorized access and improper use.

If you are unclear about any of the responsibilities outlined above, seek guidance from your direct manager.

I understand and agree to follow *[Your Organization's Name Here]*'s information security and technology use policy.

_____ _____

Employee Name (printed) **Employee Signature**

Date: _____