maestrosoft
an arreva company

Ethics and Security

MaestroSoft, Inc.
1750 112th Avenue NE, Suite A200, Bellevue, WA 98004

425.688.0809 / 800.438.6498 • Fax: 425.688.0999
www.maestrosoft.com

Contents

Internal Standards

Product Security

Ethics and Business Standards

"As a company, we become a member of society in the cities and towns in which we conduct business, and we have a responsibility to respect that with every decision we make."

A VISION FOR A BETTER WORLD

MaestroSoft is a company that empowers all employees with the rights and responsibilities of making decisions that affect our business. Our decisions shape our reputation within our industry and define us as a socially responsible company.

MaestroSoft employees are taught the corporate vision set forth by our co-founder Michael Bader - that every client is special and valuable, and we must treat our clients like the respected charities, schools, foundations, and 501(c)(3) organizations that they are. This corporate vision affects the level of service we provide and the products we offer.

As a company, we become a member of society in the cities and towns in which we conduct business, and we have a responsibility to respect that with every decision we make. Our choices play a direct role in ensuring our presence in those societies remains positive, fair, and true to our corporate vision.

COMMITMENT TO RESPECT

At MaestroSoft we treat each other with total respect and dignity. Our office environment directly impacts our personal willingness to follow the standards of client conduct. We pride ourselves with being an Equal Opportunity Employer, and will not discriminate based on race, color, national origin, religion, sex, age, sexual orientation, disability, or genetic information. Without a workplace free of discrimination, harassment, and bullying - we'll never be able to meet the corporate culture standards of respect and dignity that matter most.

COMMITMENT TO OUR CLIENTS

Our clients are at the core of all that we do. Without our clients, we have no one to support, no one to innovate new products for, and no one to support our business. Our clients have chosen us over our competitors, and we must respect that at all times.

Our conduct with our clients must remain a top priority. Listening to our clients and providing them the best level of service is what defines us as a company. Our conduct over phone and email will remain courteous and objective at all times, and in-person conduct will remain top notch with a clean and welcoming office space to make our clients feel at home.

Our products will continue to be reliable and innovative. The Feedback Portal on our company website has been put in place to capture client feedback about all parts of our business, and we will welcome comments through the portal, as well as phone, email, and in person.

COMMITMENT TO HONEST BUSINESS

MaestroSoft is committed to full compliance with the laws and regulations that apply to our business practices in all countries, states, and cities in which we do business.

We compete only on the merits of our products and services. Our advertising and sales literature will never disparage our competitors. We will never say something about our products or services if we can not substantiate it.

COMMITMENT TO IMPROVING OUR ETHICS AND BUSINESS PRACTICES

Each year, following an ethics audit, we will make improvements to our ethics and business practices. We will strive to make MaestroSoft a better company each year, and never lose sight of our clients' best interests, our ambition to innovate, and our corporate vision.

Privacy Policy

Our Website’s Privacy Policy

The MaestroSoft® web site does not collect sensitive personal information.

If you send us an e-mail with a question or comment, we will write back to you using your e-mail address. We may keep your question or comment and your e-mail address on file, but we will not disclose your e-mail address, or any personal specifics regarding your question or comment to any third party without your consent. In order to serve the community, we may include your question on a Frequently-Asked-Questions page, but should we do so we will make sure that your question will not in any way identify you.

We will send newsletters and other communications to you via e-mail only if you have NOT asked to be excluded from such mailings.

We will not sell or share any information that we collect from you. We restrict access to your personal information to company personnel only (and then, on a need-to-know basis) and have procedural safeguards in place to ensure that. We will share your information with a third party only as required to deliver products and services to you that you have requested from us.

All photos and testimonials are posted to the MaestroSoft web site after we have received explicit written permission to do so.

This website uses Google Analytics, a web analytics service provided by Google, Inc. (“Google”). Google Analytics uses “cookies”, which are text files placed on your computer, to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for MaestroSoft, Inc. and providing other services relating to website activity and internet usage. MaestroSoft does not share any of this information with outside or third party companies.

We may become an affiliate of one or more businesses. Should you follow a link from the MaestroSoft web site to an affiliate website, then you will be communicating directly with that affiliate and not with us, and you will be subject to that affiliate's privacy policy.

EU-U.S. Privacy Shield

Our Commitment to Privacy

Maestrosoft, Inc. complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States (if this situation ever occurs).

Maestrosoft, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

Our complicance to strict EU-U.S. standards ensures your privacy even if you're an organization in the United States.

To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

MaestroAuction Online Security

MaestroAuction Online uses 128-bit encryption for all password protected areas and role-based authentication.

Our database, image and web servers are physically secured in a state-of-the-art data center in downtown Seattle, where they are monitored 24/7 and a backup power supply is available. All our servers are patched with the appropriate service packs and critical updates immediately when they are available. Further, our server configurations follow security “best practices” and prohibit access through non-essential ports. In addition to physically securing the SQL Server Database, all the database queries that MaestroAuction Online uses are precompiled in stored procedures. This means that the MaestroAuction Online application itself doesn’t even have direct access to the SQL Server tables, but can only update the database by using these predefined queries.

Roles-Based Authentication

Further, MaestroAuction Online uses the .NET framework and requires sign in authentication before users have access to the password protected areas of your site. MaestroAuction Online has extended this .NET security with a role-based authentication system, which allows your site administrator to assign different levels of access among your administrative team. By default, everyone in your database is granted the “User” role and can access the public password-protected areas of your MaestroAuction Online site once they’ve created or been assigned a password. Only people who are assigned one or more of the administrative roles (“Reports”, “Items”, “Registration”, “People” or “Administrator”) will have access to the administrative tools page on your MaestroAuction Online site. They’ll then only be able to use specific administrative tools if they have been assigned the corresponding role. For example, a volunteer who has only been assigned the “Reports” role will only be able to view administrative reports, but not update items, people or event information.

Secure Transmitting

You’ll notice that when you sign in and subsequently access all password protected areas of your MaestroAuction Online site, the URL in the address bar is “https://secure.maestroweb.com/...” and there is a padlock in your browser which links to our “SSL Secured (128-bit)” certificate. Our use of 128-bit encryption for all password-protected areas assures that all the information in your database is kept completely confidential during transmission between your browser and the MaestroAuction Online server.

Secure Payment Tools

We offer online payment processing so that visitors to your MaestroAuction Online website can register for the auction dinner, make cash contributions, purchase merchandise, and/ or pay for item purchases. Each of our clients establishes an account with our payment processing partner: The payments are entered securely using MaestroAuction Online , so that the transaction can be immediately reflected in the client's event database. We securely transmit the credit card information to the payment gateway for processing and then only store the last four digits of the credit card number and authorization information in our database for reference.

Learn about IATS at: http://www.iatspayments.com

PCI Compliance

As indicated above, MaestroWeb also doesn't actually process or store credit cards.

MaestroAuction Security

Credit Card Collection Site

During the event, credit card information is collected by the qCheck Registration Utility. This utility was built by IATS (our PCI compliant Credit Card Processor). Once the credit card information is collected it is stored in an encrypted format.

This information may be stored in any or all of the following 3 locations:

- **The MaestroAuction Server** – This is the back room computer that is hosting the MaestroAuction databases. The encrypted credit card information may be backed up to this computer.
- **qCheck Registration Station** – This is a standalone laptop that is setup at the registration area . A client may setup any number of qCheck Registration Stations. The qCheck Registration Utility is setup and removed by the qCheck Station Manager.
- **qCheck USB Drive** – A USB flash drive is used transfer data from the MaestroAuction Server to the qCheck Registration Stations. This includes transferring the encrypted credit card data from the qCheck Registration Station back to the MaestroAuction server.

The IATS Server

After the event is over, it is necessary to upload the client's credit card information to the IATS server. This is done using an encrypted connection created by the IATSLink.dll (provided by IATS.) IATS is PCI Compliant, certified by TrustWave. You can verify this status by visiting http://www.iatspayments.com/english/pci_compliance.html

Once the data has been successfully uploaded to the IATS server all copies of the encrypted credit card data can be deleted.

PCI Compliance

MaestroAuction does not store any credit card data, and therefore does not need to be PCI Compliant. All information is stored by the IATS Registration Utility.

iaTS and PCI Compliance

Some words about our processing partner

IATS Payments provides payment processing products and services to over 9,000 clients around the world and specializes in services for nonprofit organizations. IATS draws on over 30 years of transaction processing experience to provide secure, simple and cost-effective services for all major credit cards and direct debit (ACH). A First American Payment Systems Company, IATS is based in Vancouver, Canada. IATS Payments was established in 1996 and is focused exclusively on providing payment processing services to the nonprofit community. Their clients are located in the United States, Canada, the United Kingdom and throughout Europe.

IATS is proud to have been issued a VeriSign certificate, which verifies that their site is SSL-secured at the very demanding 128-bit level of encryption. VeriSign issues three levels of certificate – 40, 56 and 128-bit – with the latter being the most secure level available anywhere in the world. The number of "bits" describes the length of the key used to secure the encrypted information. While the difference between 40 and 128 bits of encryption may not sound impressive, it is very significant. 128 bit keys are approximately 309 septillion times (309,485,000,000,000,000,000,000,000) larger than 40-bit keys. This high level of encryption makes breaking into an SSL session extremely difficult. If you happened to have a million computers testing a million possible keys every second, it would still take over 10 million years to test every combination and permutation available – and that is only for 40-bit encryption; 128-bit SSL sessions are much more difficult to break.

They do not, however, release information regarding the measures they use to keep their system secure to ensure this information can not be abused. IATS considers all personal information as confidential and they do not disclose personal information to any third parties. All employees of IATS with access to personal information are required as a condition of employment to respect the confidentiality of personal information.

Also, IATS completes an annual audit process from a third party to verify they abide by the rules and regulations of the payment card industry standards. This is to ensure they can provide our mutual clients with the highest levels of security and fraud prevention. They are a **Level 1 PCI Compliant** company and this can be verified on the Visa website by using the following link. This will give you access to a listing of all the companies and merchant service providers who are PCI compliant.

http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp