U.S. Coast Guard TRACEN Petaluma

Morale, Well-Being & Recreation

Online Security Plan

Points of Contact

Mr. Michael Criswell, Director

Michael.A.Criswell@uscg.mil

707.765.7343

Tameron Eaton

Marketing & Sponsorship

Tameron.A.Eaton@uscg.mil

707.765.7261

Accepting Online Payments

The website host we currently use is Wix.com. The online shopping cart we use is Ecwid.com and the payment gateway we use for our online store is Payeezy.com. Both seamlessly integrate with the Clover point of sale (POS) systems, standard across Coast Guard (CG) MWR programs globally. These products also integrate seamlessly with First Data, the payment processor standard across CG MWR programs. These are key points for future web and POS integration providing us the ability to expand beyond this proposed website 2.0 project looking forward to website project 3.0 at a later date.

Online Payments Security

For websites running managed stores like Wix.com, the server and all its software are proprietary. This means the website owner is not held liable for security configurations, and we pay the service provider a monthly fee for this luxury.[1]

Ecwid.com – Online Shopping Cart

Ecwid complies with the EU-US and US-Swiss Privacy Shield Frameworks as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Ecwid has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.[2]

Payeezy.com – Payment Gateway

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We maintain annual compliance with global Payment Card Industry Data Security Standard (PCI DSS) adopted by the payment card brands for all companies that process, store or transmit cardholder data.

[1] https://blog.sucuri.net/2017/09/intro-to-securing-an-online-store.html

[2] https://www.ecwid.com/privacy-policy

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach…[3]

Website Security

Hyper Text Transfer Protocol **Secure** (HTTP**S**) is the secure protocol through which your browser communicates with sites. When using HTT**P** sites, any data that is transferred can potentially be accessed or manipulated by attackers. However, when using HTTP**S** sites, data is encrypted and authenticated and therefore secured. Our Wix.com site utilizes HTTP**S**.

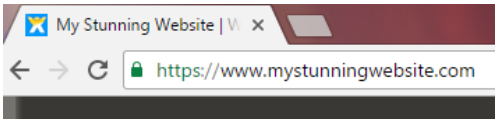
Benefits of Using HTTPS

1) Our site visitors' information is encrypted and therefore more secure.
2) Many users are more comfortable making purchases and sharing their personal information online when visiting secured sites.
3) Some web browsers like Google Chrome now display warnings anytime a user visits a site that is not using HTTPS. Therefore, if your site is not secured, your site visitors will get a warning message anytime they access your site.
4) Google ranks HTTPS sites more favorably. Having a site using HTTPS improves our Search Engine Optimization (SEO) causing our site to appear higher in search results which drives more traffic to our site.

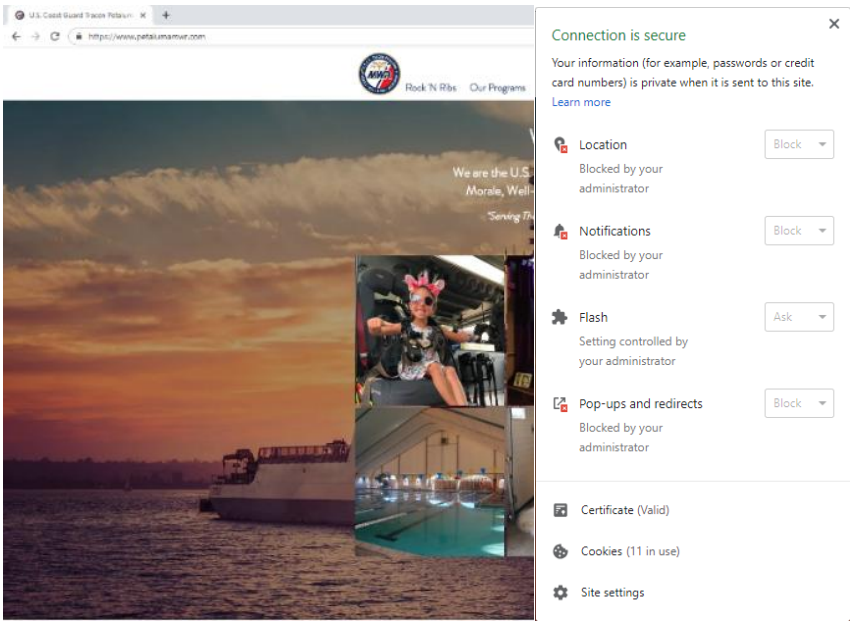
To prevent unauthorized access, promote data security, and encourage appropriate use of information, Wix uses a variety of tools, such as encryption technologies, passwords, physical and electronic security, or procedural safeguards to assist in the protection of your information.

What is an SSL Certificate?

A Secure Sockets Layer, or SSL certificate, allows our site visitors to view our site over an HTTPS connection. It secures the connection between their browser and our site. Wix provides our site with an SSL certificate. We can see that our site has an SSL certificate as our URL begins with https:// instead of http://. A site without an SSL certificate shows an "i" icon in browsers such as Google Chrome.



[3] https://www.firstdata.com/en_us/privacy.html#row8



Wix Certifications

PCI Compliance

Every business that handles credit card information (including storing, processing, and transmitting cardholder data) must be PCI compliant. To ensure credit data remains as secure as possible, the PCI Data Security Standard (PCI DSS) offers a guideline with 12 central security areas—these are identified as the minimum level of security measures organizations need to take.

PCI compliance involves a contractual agreement with acquiring banks, and some U.S. states have introduced elements of PCI compliance into their own laws. Ultimately, responsibility for any breaches falls upon the hotel.[4] Wix is Payment Card Industry Data Security Standards (PCI DSS) compliant and is accredited as a level 1 service provider and merchant. The PCI DSS is an information security standard for organizations or companies that accept credit card payments. This standard helps to create a secure environment by increasing cardholder data, thus reducing credit card fraud.

ISO Compliance

ISO is an independent, non-governmental international organization Certification can be a useful tool to add credibility, by demonstrating that your product or service meets the expectations of your customers. For some industries, certification is a legal or contractual requirement.[5]

ISO 27001 Compliance

Wix has been audited and certified as ISO 27001 compliant. The ISO 27001 certification outlines industry best practices for managing security risks.

[4] https://www.traveltripper.com/blog/hotel-data-security-understand-the-difference-between-pci-and-pii-compliance/

[5] https://www.iso.org/home.html

CERTIFICATE

This is to certify that the
ISMS which supports the protecting of PII in public clouds of

WIX.COM

40 Ha'namal St. , Tel Aviv , Israel

Has been audited and registered by SII-QCD as conforming to the requirements of :

ISO 27001:2013 And ISO 27018:2014 Best Practices

This Certificate is Applicable to

Developing, marketing, provisioning and support of web sites self development platform. Hosting of customers web sites in the company production DCs, information security incident response preparation.

Certificate No.: 80992
Initial Certification Date: 22/06/2016
Certificate Issue Date: 22/06/2017
Certification Expiry Date: 21/06/2019

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement.
This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Pinhas Shaher
Director General

Eli Cohen-Kagan
Director, Quality & Certification Division

Page 1 of 1

Our Vision: To Enhance Both Global Competitiveness of our Services, with our Uncompromised Quality and Integrity

ISO 27018 Compliance

Wix has been audited and certified as ISO 27018 compliant. The ISO 27018 certification outlines industry best practices for handling personally Identifiable Information (PII) in a public cloud computing environment.

TLS Certification

Wix uses Transport Layer Security (TLS) encryption to help protect all of our online financial transactions.

Capturing, using and storing customer data

Customer Information

There is nothing more important to this project that capturing, using and respecting our users information. In order for our website to progress to the next necessary step we need to create the ability to receive PII and SPII from customers through our website, use it internally within our programs following the applicable policies and regulations, and store said information in our secure shared Coast Guard email MWR@uscg.mil.

Definitions

Privacy Act Statement

Purpose: To allow MWR eligible individuals to reserve USCG MWR facilities and equipment or participate in USCG MWR sponsored events, contests or programs.

Routine uses: USCG MWR personnel will use this information to determine an individual's eligibility, validate reservations, and verify results of USCG MWR events.[6]

Department of Homeland Security (DHS) defines personal information as "Personally

[6] 10 USC 1146 and 14 USC 93, 487

Identifiable Information" or **PII**, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department. PII is a form of Sensitive Information, 1 which includes, but is not limited to, PII and Sensitive PII. Sensitive PII (**SPII**) is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised. Some categories of PII are sensitive as stand-alone data elements, including your Social Security number (SSN) and driver's license or state identification number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII. [7]

Applicable DHS Fair Information Practice Principles (FIPP)

Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.[8]

IT Systems: Once collected, SPII should be stored based on the specifications for either electronic or paper storage outlined in the SORN, if necessary and applicable, under the

[7] Handbook for Safeguarding Sensitive PII, DHS, 4 December, 2017.
[8] Handbook for Safeguarding Sensitive PII, DHS, 4 December, 2017.

section titled: Policies and Practices for Storage of Records. Databases or IT systems storing SPII should employ technical safeguards and access controls to restrict access to staff with an official need to know the Sensitive Information.

Do not send emails containing SPII to or from your personal email account, or to another person's personal email account.

Internally you are authorized to share SPII with other DHS staff only if the recipient has an official need to know, and/or the person whose SPII is being shared consents to the sharing.

Best practices

- Minimize Dissemination of SPII Whenever possible, minimize the duplication and dissemination of electronic files and papers containing SPII.
- Only print, extract, or copy SPII when there are no other means of disseminating the data.
- Before emailing, printing, or copying, redact SPII that is beyond the scope of the data request or is not appropriate for the requestor to have.

Email Internally

- DHS policy permits emailing SPII within the DHS network without encryption or password -protection to a recipient with an official need to know.

Note: If someone outside of DHS sends you SPII in an unprotected manner, you must protect that data in the same manner as all SPII you handle once you receive it. For example, if someone outside of DHS sends you unsecured SPII in the body of an email, you must delete the SPII from the body of the email, put it in a separate attachment, and encrypt or password-protect the data if you wish to respond to that individual or email it to another recipient outside the dhs.gov domain. Alternatively, you can redact the SPII before responding to or forwarding the email.

You should periodically review the hard copy and electronic SPII in your possession to determine if it is still needed, especially prior to an office move or when leaving the agency. SPII, including that found in archived emails, must be disposed of when no longer required. [9]

Email Security

Department of Homeland Security Policies

CG unclassified e-mail service provides a secure means to transmit e-mail between "USCG.MIL" and "DHS.GOV" accounts for delivery of official CG correspondence to include SBU information, For Official Use Only (FOUO), Critical Information List (CIL),

[9] Handbook for Safeguarding Sensitive PII, DHS, 4 December, 2017.

Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), and Public Health Information (PHI).

E-mails containing sensitive information (including but not limited to: PII, SPII, PHI, or CIL) may be sent freely across the DOD.MIL and DHS.GOV domains without encryption, if the recipient's need for the information is related to his or her official duties. However, if you have any doubt about that need, or to provide an additional layer of protection, it is strongly recommended that you encrypt the e-mail containing the sensitive information.[10]

Conclusion

We have established the business need and clearly outlined the standard operating procedures that when followed will ensure beyond a reasonable doubt the security of our customers information. Our Wix.com website, Ecwid and First Data all have Level 1 security as verified by numerous third party audits. The three companies are certified PCI compliant. Our Coast Guard email account and server offer the highest level of security and encryption. Existing DHS and DOD policies allow for the capture, use and safe storage of PII and SPII. The policies, security measures and best practices outlined in this document are applicable for all of the actions we wish to undertake in this website project.

[10] DHS COMDTINST M5500.13E