WordPress Site Security

iDiz Incorporated
Updated November 2024

Getting Support

Who should I contact if there's a problem with my website or I have a question?

For all issues with your site, please contact iDiz Incorporated directly:

- During business hours, call iDiz Incorporated at **317.257.0000**
- You can also email **support@idizinc.com** at any time. Messages sent to this email address are automatically flagged as urgent and forwarded to our entire team.
- If you have an urgent issue after hours, call or text **765.714.2761**.

What kind of response can I expect?

As you can see, we approach support very personally and very seriously. You can expect a response very quickly, and most issues will also be resolved within 24 hours. If a resolution will take longer, we will update you as soon as possible, and stay in touch until the issue is resolved.

Introduction

Website security is a highly technical, complex and constantly changing topic, and there are many interlocking layers to any security plan.

In this document, we'll outline how we manage these factors, and clarify the following:

- How your site and the WordPress software are kept safe and secure
- What the risks are
- Your responsibilities regarding your site's security, stability, and performance
- What you should do and what you can expect if there's a problem

We strive to avoid technical jargon as much as possible so that this document will be clearer and more understandable to more people, and thus a more useful part of your planning and preparedness.

This document is reviewed a minimum of twice per year, and updated as needed. Feedback from our clients and from their contacts with regulators is very important. We rely on your feedback to improve the usefulness and clarity of this document as well as the security, reliability, performance, and usefulness of your web site.

If you have any further questions regarding iDiz Incorporated or this document, please email **support@idizinc.com**

What are the Risks?

It's important to understand that there's no such thing as absolute website security. By offering a website to the world, certain risks are inevitable. The approach, as with any other aspect of doing business, is to manage these risks to keep them at a minimum. Some of the risks related to financial institution websites include:

- **Fraud risk** - although our sites never handle transaction data, an attacker who gained access to your site could change the site and use the site to mislead staff or users.
- **Reputation risk** - if a site is vandalized, defaced, unreliable, or altered, it could affect your reputation and credibility.
- **Downtime** - an attacker or event (for example, a DDoS attack, disaster) that causes your site to be unavailable can cause inconvenience for you and your staff or users.
- **Damage to others** - a compromised site could be used to spread malware or viruses.

Is WordPress Safe?

WordPress is by far the world's most popular Content Management System (CMS). Over 43% of all websites are built with WordPress, and ⅔ of the sites built with a CMS are built with WordPress. WordPress is used by many Fortune 50 and Fortune 500 companies, including many financial institutions.

Like any powerful software, WordPress can be used safely, or it can be misused and neglected and cause problems. And like any software, WordPress and its plugins also require monitoring and timely updates in order to stay safe. In much the same way, Microsoft Windows is the most popular computer operating system, and thus is the most attacked. However, Microsoft Windows can be used safely as long as it's kept updated and is monitored and managed properly.

You may have seen reports of websites using WordPress that have been hacked. In every case we're aware of, the website was simply not maintained properly -- these attacks could have been easily prevented by keeping WordPress and the site's plugins up to date and monitoring activity.

How are the WordPress software, my website, and the server environment kept safe and reliable?

At iDiz Inc., we employ multiple layers of monitoring and WordPress management, including monitoring for malware, uptime, response time, and many other factors. We also have additional automated daily backups made to a different location, and we employ software that monitors WordPress and any plugins and keeps everything up to date. Monitoring is in real-time, and we receive daily reports, as well as instant alerts if needed.

Our WordPress sites are hosted with a company based in Austin, Texas called WP Engine. WP Engine is the first and largest company to specialize exclusively in high-security, high reliability Managed WordPress Hosting, and they currently host over 1.5 million sites. WP Engine is responsible for managing, updating, backing up, securing, monitoring, and maintaining the WordPress software as well as the server environment (OS and server software).

WP Engine buys its infrastructure (raw computing, storage, and bandwidth) from several different providers. The data center housing the WordPress sites we build is physically located near Council Bluffs, Iowa, and is operated by a division of Google called Google Cloud (https://www.google.com/about/datacenters/locations/council-bluffs/). Google Cloud provides internet infrastructure to millions of the world's largest companies, including thousands of banks and credit unions. Google Cloud handles the safety, security, and availability of the physical and software infrastructure -- the network, servers, OS, monitoring, and physical security.

WP Engine has started transitioning to an Advanced Network system from Cloudflare. In a nutshell, this offers increased security, speed, and stability for sites hosted with WP Engine. Since late 2022, our new sites have been launched with Advanced Network in place, and existing sites are in the process of transitioning. This requires making a few DNS updates, and we are working with our clients to complete the upgrades as soon as possible. You can find more information here: https://wpengine.com/support/advanced-network/

Where can I get more information about the security environments of WP Engine and Google Cloud?

We encourage you to view the following links and browse the WP Engine and Google Cloud websites to gain a greater understanding of the high quality and integrity of their services.
Google Cloud: https://cloud.google.com/security/compliance
WP Engine: https://wpengine.com/support/wp-engines-security-environment/

You can find Google Cloud's SSAE18 and SOC reports and other documentation here:
https://cloud.google.com/security/compliance/compliance-reports-manager
Filter by reports pertaining to Google Cloud and the "Global" region.

How do you keep account data, transactions, and sensitive personal information safe?

We maintain a strict policy of separation between the sites we build and your transaction systems – **we never store, transmit, or process member data, account data, or transaction data in our systems.**

If you need to collect such data, you do have the option of using embedded forms from a secure encrypted form processor such as Formstack, Documatix, Docusign, Cognito Forms, Microsoft Forms, and others. These can be seamlessly embedded in pages, but the actual data never passes through our systems.

If you choose to use a secure forms provider, you will create and own the account so that ownership and access to your member data is never in question. With some of these systems, we can be added as users to help build forms without having access to your member data, and we're happy to do so.

In much the same way, you might have login forms for online banking or other systems on your site, but the user or transaction data is never transmitted to or through your site or displayed in your site; the form communicates directly with the online banking systems.

We monitor WordPress user signups and logins, and manage user access levels to minimize access risks. All user activity is logged. In addition, we follow personal verification procedures before making changes at your request.

Our practices and technologies are very secure – on a level appropriate for a transactional website – but maintaining a strict data separation policy helps ensure that our clients' websites do not become specific targets for theft or attack. This also helps ensure a consistent experience for your members; member transactions and member data are always handled via the appropriate systems.

Does my site use SSL?

Yes. All the sites we build use SSL. Using SSL helps reassure users that your site is safe, and allows all connections within WordPress to be encrypted so that usernames and passwords are secure.

WP Engine uses Let's Encrypt and CloudFlare automated SSL certificates to offer the most up to date levels of encryption. These SSL certs renew automatically, so there are never any worries about expiration or renewal.

Note that automated SSL certificates renew on a specific schedule with a timeframe much shorter than traditional manual certificates which are renewed annually. If you have systems in place that monitor for SSL renewal, you may need to adjust the settings or remove the monitors.

Does my site login include Two-Factor Authentication?

Your site's login to WordPress is very well-protected in several ways; strong passwords are enforced, logins are rate-limited, and logins are closely monitored for suspicious activity. If you'd like to add 2FA (Two-Factor Authentication) we're happy to do so. 2FA using an Authenticator app (with backup codes) can be added at no charge, and most Authenticator apps are supported. 2FA with email or SMS options will entail added setup and maintenance costs; please get in touch for details.

Our logins to the hosting controls are secured with 2FA.

How do backups work?

Your site is automatically backed up every evening by WP Engine. In addition, we have a second backup process in place that makes a second backup of your site every day to an entirely different data center.

We also have the ability to quickly generate a backup "snapshot" at any time. This is routine before installing new plugins or changing certain settings. Approximately 40 backups (including both daily and on-demand backups) are retained, and we can revert to any WP Engine backup in a few minutes.

What if something really, really awful happens to iDiz?

Your website would be safe. Since your WordPress installation and your site are hosted in a highly secure data center in a different location, a disaster at iDiz Incorporated would not threaten the stability or availability of your site.

If you need to work with other developers temporarily, WordPress is very well known. You have Admin access to the site, and you can add and manage users.

If the need arises, WP Engine's Support has a process for verifying domain name ownership and working directly with domain name owners.

How do we include our website in our disaster recovery plan?

Your website can and should be a valuable part of your disaster recovery planning.

Your site is not hosted on your premises or ours and you can access your site with any computer with an internet connection (it's not tied to certain software installed on certain computers).

This means your website will not be affected by a crisis at your location. Staff can update the website easily and quickly, so it's an important tool for communicating with account holders, the public, and other staff in a crisis.

In addition, you do not need to maintain, protect, secure, repair, replace, or restore a physical in-house or remote web server, so many of the IT and disaster recovery costs related to your website are eliminated.

Do you archive site content changes?

In order to maintain performance and reasonable hosting costs, site content changes are not archived, and the daily site backups are only kept for 30-40 days. If you require an archiving function, there are several third-party services available; contact us for more information.

My compliance officer and/or vendor management provider needs more information, documentation, or forms filled out.

We're happy to work with your compliance and vendor management personnel to address any concerns or answer questions. This feedback is a valuable part of our process of maintaining security and keeping this document updated so that all such questions are answered in one place.

If additional time is needed or expenses are incurred for filling out lengthy online forms, obtaining added documentation, or researching answers for compliance or vendor management, we will track the time and expenses and invoice at our standard rate.

Can we have our site's security evaluated by our IT or security vendor?

Yes, with a few conditions:

- Let us know that you plan to test, and approximately when
- Share the results with us
- Avoid testing that could negatively affect your site or our hosting environment
- Take responsibility for any consequences of the testing. For example, clients who have simulated suspicious activity in the past have found their IPs quickly blocked by WP Engine or Cloudflare.
- Understand that our hosting environment is highly customized and optimized, and may return unexpected results. For example, scanning for well-known vulnerabilities will often return obfuscated or nonsense results; confusion is more effective than blocking.

If extensive research, detailed responses, changes, or fixes are needed, we may track and invoice time and expenses at our usual rates.

Can I add an Accessibility "overlay" plugin or script to my site?

We do not allow overlay plugins or scripts to be installed on the sites we manage. There are several reasons for this.

- **Overlays are simply not needed.** We build sites with excellent Accessibility, train our clients in maintaining a high level of Accessibility, and we offer the option for regular Accessibility audits. More info: https://www.cuidiz.com/what-we-do/accessibility-services/

- **Overlays actually make real-world Accessibility worse** by interfering with the settings, tools, and software used by people who need them.

- **Overlays degrade the user experience for everyone.** By loading and running a very large JavaScript and other assets, sites slow down and the overlay interfaces often interfere with the site's actual interface by making unpredictable changes to the site.

- **Overlays create serious privacy and security concerns.** Most such scripts depend on third-party servers with security and privacy practices that are unknown and can change, and private user data (such as information on a user's disability) may be tracked via cookies or sent to third-party servers.

Here are a few links to better understand these issues, directly from respected Accessibility experts:

- https://overlayfactsheet.com/en/
- https://www.a11yproject.com/posts/should-i-use-an-accessibility-overlay/

Some of the most common examples of these problematic overlays are UserWay, AccessiBe, and AudioEye, but there are many others.

What responsibilities do I have for keeping my site safe?

Of course, all the technology in the world can't protect against social engineering or poor user management. As our client and as a WordPress user, you have several important primary responsibilities for keeping your site safe:

- **Keep your WordPress account information (usernames and passwords) secret and secure.** Strong passwords are required. Treat your WordPress logins with the same level of secrecy and care that you use for your transaction systems. Never tell anyone your password (not even someone claiming to be from iDiz), never write it down, and never store your password in plain text. You may use password management software as long as it meets your institution's standards for use with your transaction systems.

  Remember: no one will ever ask for or be able to see your password. WordPress passwords are encrypted and stored using a "one-way" encryption method -- this is a mathematical method that makes it impossible to reconstruct a password from its encrypted form. If you lose or forget your password, you can reset it, but no one can see, reproduce, or recover any password.

  A note about password resets: when you or an Admin user reset your password, it's quite common for the email from WordPress to end up caught by your spam filter. Make sure you check your filter if you didn't get the reset email. If that doesn't work, contact us for assistance (see first page).

- **Consider adding 2FA** to your login process as outlined above.

- **Contact iDiz Inc. immediately** if you feel there may have been a compromise.

- **If someone leaves or changes roles, immediately remove or update their access,** just as you would for access to your email or transaction systems. We are happy to assist with this if needed. We verify all such requests to make sure they are authorized.

- **Do not share WordPress user accounts – each person must have their own account.** This also helps ensure that passwords are not shared or written down. We do not limit the number of user accounts.

- **Always communicate with iDiz Inc. before adding new users to arrange training and orientation.** Even people who are very experienced with WordPress MUST be oriented to the way your particular site works and how it was built. This applies to both staff and any third-party providers such as content creators, SEO consultants, etc.

- **Create user accounts with the minimum level of access needed.** WordPress gives you the ability to restrict user roles. Think carefully about who has access to what, and give out only the access privileges that are needed.

- **Always check with iDiz Inc. before adding plugins, scripts, or any third-party code to your site.** Third-party code or additional WordPress plugins are often necessary and useful (for example, many online banking logins, branch maps, and forms use embedded iframes or Javascripts), and plugins add important functions.

  But before adding anything to your site, we need to review and test code and plugins. We need to make sure we understand exactly what the code is doing, that it comes from a trusted provider, that it integrates smoothly with your site, that it enhances your brand and user experience as expected, and that it does not impact stability, performance, Accessibility, privacy, security, or usability. In some cases, we can suggest a more usable or stable solution.

  We are happy to help test and assess code and plugins when needed, or assist you with interfacing with other providers.

- **Do not collect, process, or store member information within the site**. As outlined above, we maintain a strict policy of separating member data from the sites we build. If you need to collect this data, use a secure forms provider and embed the forms within your site.

- **Plan regular review and "sunsetting" of third-party code.** Many times, third-party code is useful for implementing or tracking things like marketing campaigns. When adding this to your site, set a date and a calendar reminder for review and removal.

- **Use the minimum necessary level of tracking.** Balance your credit union's need for data and analytics to improve effectiveness and the user experience against your members' expectations for privacy and security.

SUMMARY: Layers of Security and Reliability

Layer:	Responsibility:	Responsible For:
WordPress Users	Client, iDiz	User activity, passwords, user access levels.
Site Stability & Performance	Client, iDiz	User configuration and training, vetting plugins, third-party code & users
External Monitoring	iDiz	Additional monitoring for uptime, malware
Offsite Backups	iDiz	Daily offsite backups
Updates	iDiz, WP Engine	Monitoring for updates, applying and testing WordPress and Plugin Updates; security-related updates are applied immediately
WordPress Instance	WP Engine	Optimization, Downtime, attacks, testing, malware monitoring, activity monitoring, recovery, Nightly and ad hoc backups, Logins and user activity closely monitored and limited
Server software	Google Cloud, WP Engine	Downtime, attacks, malware, server activity, updates
OS (Linux)	Google Cloud	Downtime, attacks. Updates, patches
Network, Routing	Google Cloud, WP Engine, Cloudflare (Advanced Network)	DoS attacks, hardware failures, optimization
Physical	Google Cloud	Physical access, intrusion, power backup, hardware security and reliability,

Legal and Liability

Ownership and Rights
Website design and content become the property of Client upon final and full payment.

What if I want to move my site in the future?
No problem, although we'd hate to see you go! You own and control your domain name and site content, and you may move your website at any time. Upon request, iDiz Incorporated will export the site files and database, and provide the information needed for another developer to install the site on another WordPress instance and relicense any plugins. We will make every reasonable effort to ensure a smooth transition.

The actual time involved in providing these files and coordinating the transfer will be billed at our usual hourly rate. Relicensing costs and other costs related to setting up your site with a new provider are not included.

Likewise, if iDiz Inc. ever decides to terminate the agreement, we will provide at least 30 days notice, we will provide the site materials and information as above free of charge, and we will make every reasonable effort to coordinate a smooth transition.

What kinds of actions could iDiz Inc. and WP Engine take to keep our site safe?
In order to maintain the security, stability, and performance of your site and our hosting environment, iDiz Inc. and WP Engine, at their discretion, may take action including but not limited to: reverting or removing changes, disabling or removing plugins or code, disabling or removing features, disabling or removing users, restricting user access, additional verification of requested changes, and other actions as needed.

If these actions could affect the user experience, we will provide advance notice where practical, and we will keep you informed via email whenever such action is needed.

What happens if our site goes down?
If your website is not available for a period of time exceeding 30 minutes, iDiz Inc. may, at its sole discretion, offer a prorated refund or credit for that time period's Hosting and Support costs.

Dispute Resolution
Should there be a dispute, both parties agree that they will attempt to resolve problems in an expeditious manner, as well as make reasonable efforts to provide for continuation of services during the resolution period.

Limited Liability
In no event shall either party be liable to the other for any indirect, special, exemplary or consequential damages, including any implied fitness for a particular purpose or implied

warranties arising from course of dealing or course of performance, lost profits, whether or not foreseeable or alleged to be based on breach of warranty, contract, negligence or strict liability, arising under this agreement, loss of data, or any performance under this agreement, even if such party has been advised of the possibility of such damages and notwithstanding the failure of essential purpose of any limited remedy provided herein. The maximum remedy available to either party is any amount paid by customer hereunder. iDiz Inc. makes no warranty of any kind, whether express or implied, with regard to any third party products, third party content or any software, equipment, or hardware obtained from third parties.

Recent Changes to this Document

9/2023

- Added more details on Let's Encrypt automated SSL certificates
- Added more details on Advanced Network/Cloudflare
- Added third-party code sunsetting language
- Added requirement for new user orientation/training
- Added information about some of the possible actions iDiz may take to ensure safety, stability, and performance of individual sites and our hosting environment
- Clarified ownership
- Clarified language about third-party users and access levels.
- Clarified language about storing sensitive personal data
- Clarified language on third-party plugins and code
- Clarified Layers of Security information
- Moved Support contact information to the top
- Added information on archiving services

6/2024

- Clarified Advanced Network info
- Clarified Cloudflare's role

11/2024

- Clarified language about member data
- Added details about automated SSL certificates via Let's Encrypt and Cloudflare
- Added details about accessing Google Cloud SSAE/SOC reports
- Clarified handling of added time and expenses for compliance/vendor management
- Added information about 2FA options
- Clarified termination terms
- Added information about security testing
- Added information about Accessibility overlays