Standard Operating Procedure (SOP) for WordPress Website Security Protocols

Document Control

- **Version:** 1.0
- **Date:** 04/08/2024
- **Document Owner:** Judd Dunagan
- **Approval:** Judd Dunagan, Mihai Domocos, Romina Bocon

Purpose

This SOP outlines the security protocols for managing WordPress websites to protect against unauthorized access and potential security threats. The primary focus is on enabling two-factor authentication (2FA) and preventing passwords from being saved in browsers.

Scope

This procedure applies to all staff members managing, maintaining, or accessing the WordPress website backend.

Responsibilities

- **Website Administrators:** Responsible for enforcing security protocols.
- **IT Security Team:** Provides support and oversight of implementing security measures.
- **All Users:** Comply with security protocols.

Procedure

1. **Two-factor authentication (2FA)**
    - **Implementation:**
        1. Install and activate a 2FA plugin, such as "Two Factor Authentication" or "Wordfence Security".
        2. Navigate to the plugin settings and enable 2FA for all user roles.
        3. Choose the preferred 2FA method (e.g., email, SMS, authenticator app) and configure accordingly.
    - **User Enrollment:**
        1. Inform all users about the 2FA requirement through an official communication.

        2. Provide a step-by-step guide or training session on setting up 2FA.
        3. Set a deadline for all users to enable 2FA on their accounts.
    - **Compliance Monitoring:**
        1. Regularly review user accounts to ensure 2FA is enabled.
        2. Address any compliance issues or user difficulties promptly.
2. **No Passwords Saved in Browsers**

    - **Guidelines:**
        1. Educate users on the risks of saving passwords in browsers.
        2. Encourage the use of a secure password manager for storing passwords.
        3. Implement technical solutions to block password saving in browsers, if possible.
    - **Compliance:**
        1. Conduct periodic audits to ensure compliance with this policy.
        2. Provide support and alternatives to users for secure password management.

Additional Best Practices

- **Regular Updates:** Ensure WordPress core, themes, and plugins are updated regularly.
- **Strong Passwords:** Enforce the use of strong passwords for all accounts.
- **Limit Login Attempts:** Install a plugin to limit login attempts and block IP addresses after repeated failed attempts.
- **User Role Management:** Assign the minimum necessary permissions for users to perform their duties.
- **SSL Certificate:** Use an SSL certificate to encrypt data transmitted to and from your website.
- **Website Backups:** Schedule regular backups of your website and store them securely.
- **Security Audits:** Conduct periodic security audits and penetration testing to identify and address vulnerabilities.

Website Documentation Requirement

- **Policy Statement:** Each team member is required to maintain a detailed document for each WordPress site they manage. This document serves as a comprehensive record that includes, but is not limited to, the following information:
    - **Plugins:** A list of all installed plugins, their purpose, and the date of the last update. This section should also note any customizations or specific settings relevant to the operation of the plugin.
    - **Current Users:** A current roster of all users with access to the WordPress backend, including their roles and the date they were added. Regular audits should be conducted to ensure that only authorized users have access.
    - **Security Measures:** Any specific security measures implemented on the site, including 2FA setups, SSL certificates, and custom firewall rules.
    - **Manual Monthly Scans:** A log of manual monthly scans conducted using Immunify or a similar tool, including the date of the scan and any findings or actions taken as a result.

    - **Change Log:** A detailed change log of any updates, modifications, or significant actions taken on the site, including the date and the person responsible.

Plugin Installation and Management

- **Policy Statement:** Under no circumstances will any team member install, update, or remove plugins without express written permission from a designated authority within the organization. This policy is in place to prevent unauthorized changes that could compromise site security or functionality.

    - **Exceptions Process:** Requests for plugin installation or updates must be submitted in writing to the designated authority, including a justification for the request and an assessment of any potential security implications.
    - **Prohibited Plugins:** Using file manager plugins or any plugin known to pose security vulnerabilities is strictly prohibited. This includes but is not limited to, plugins that allow direct file manipulation within the WordPress dashboard.

Compliance and Enforcement

- **Monitoring and Audits:** Regular audits will ensure compliance with this SOP. This includes reviewing website documentation for completeness, verifying the authorization of installed plugins, and ensuring that manual scans are conducted as required.
- **Non-Compliance:** Any deviations from this SOP will be addressed immediately. Non-compliance may result in disciplinary action, including revocation of website access privileges and potential termination of employment.

Training and Awareness

- **Regular Training:** All team members will receive regular training on this SOP, including the importance of security in website management, the process for plugin installation requests, and how to conduct effective manual scans.
- **Awareness Campaigns:** Ongoing awareness campaigns will reinforce the importance of following security protocols and keeping detailed documentation of website management activities.

Secure Web Connection Requirement

Policy Statement

To ensure the highest level of security and protect against unauthorized access and potential security breaches, all team members must access the WordPress backend or conduct any website management activities over a secure web connection. Public internet connections, which are inherently insecure and vulnerable to interception, are strictly prohibited.

Secure Connection Guidelines

- **VPN Use:** When accessing the website remotely, users must utilize a Virtual Private Network (VPN) to ensure that their connection is secure and encrypted. The IT department can provide recommendations for approved VPN services.
- **Wi-Fi Security:** For those accessing the site from home or private networks, ensure that the Wi-Fi network is secured with WPA2 or WPA3 encryption and that the network password is strong and unique.
- **Public Network Prohibition:** Under no circumstances should any team member use a public Wi-Fi network (e.g., coffee shops, libraries, hotels) to access the WordPress dashboard, perform updates, or manage content. This includes tethering through public Wi-Fi networks.

Compliance and Enforcement

- **Monitoring and Detection:** The IT security team will implement monitoring solutions to detect and alert on any attempts to access the website management tools from insecure or public networks.
- **Disciplinary Actions:** Any team member found to be in violation of this policy will face immediate disciplinary action, up to and including termination of employment. This strict enforcement is necessary to protect the integrity and security of our digital assets.

User Responsibility and Reporting

- **Personal Accountability:** All users are personally responsible for ensuring the security of their web connection while accessing the website's backend. Ignorance of the policy or technical challenges will not be considered valid excuses for non-compliance.
- **Incident Reporting:** Users are encouraged to report incidents where secure web connection protocols may have been breached, intentionally or unintentionally. Prompt reporting can help mitigate potential security risks.

Training and Awareness

- **Ongoing Education:** The organization will provide ongoing education and resources to all team members on securing their internet connection, the risks associated with public networks, and how to use VPNs effectively.
- **Security Awareness Campaigns:** Regular awareness campaigns will be conducted to reinforce this policy's importance and keep all team members updated on best practices for maintaining a secure web connection.