bizTech

WEBSITE SECURITY CHECKLIST

1. WEBSITE RISK ASSESSMENT – PREPARE

□ Identify risks by assessing current security measures, including users, password strength, devices, permissions, etc.

□ Analyze current security applications used for the website.

□ Identify trusted business partners with access to your website.

□ Determine critical information that, if compromised, could harm employees, customers, or partners.

2. PROACTIVE MEASURES

□ Regularly update and patch underlying technology stack (e.g., WP Core, PHP, Plugins, Themes).

□ Enforce strong authentication practices, including MFA and access control whenever possible.

□ Encrypt data in transit (HTTPS) and sensitive data at rest.

□ Educate users and staff about security best practices.

3. ONGOING MONITORING AND DETECTION

□ Perform regular security scans and vulnerability assessments on the website.

□ Utilize reputable security scanning tools to identify and address potential weaknesses.

□ Establish real-time monitoring and intrusion detection systems.

□ Set up alerts and notifications for suspicious activities.

4. DATA PROTECTION AND RECOVERY

□ Implement automated and regular website backups with offsite storage.

□ Develop a clear incident response plan for security incidents.

□ Test backup restoration and disaster recovery processes.

□ Encrypt sensitive data stored in the website's databases, including user credentials.