Self-Assessment

Website & IT Infrastructure Security Self-Assessment

Greenhat's Website & IT Infrastructure Security Self-Assessment consists of a detailed 20-question survey, designed to evaluate the health of your website. For each question, rate your website's performance on a **scale from 1 to 5**. Your total score, out of a possible 100, indicates the overall health of your website across various essential dimensions. Importantly, **any individual dimension scoring 3 or lower should be flagged for immediate attention**. Prioritise addressing these areas, particularly those with the lowest scores, to ensure optimal website security.

	Statements	Rating
1	**User Access and Credential Management** We ensure each staff member has unique credentials to access our IT infrastructure. These credentials provide only the necessary access for each role and are regularly updated.	
2	**Network Security and DDoS Protection** Our network is protected by a firewall (e.g., Cloudflare) against DDoS attacks, and we regularly evaluate the effectiveness of our network security measures.	
3	**Payment and Sensitive Data Security** We regularly rotate security keys for our payment processing software (e.g., Stripe) to maintain high security for financial transactions.	
4	**Data Encryption and Transmission Security** We implement data encryption both at rest and in transit, ensuring secure data transmission at all times.	
5	**Regular Security Audits, Compliance, and Penetration Testing** We conduct regular security audits, compliance checks, and penetration testing to proactively identify and fix security weaknesses.	
6	**Incident Response and Disaster Recovery** We have a documented incident response and disaster recovery plan, ensuring preparedness for IT security incidents.	
7	**Employee Training and Awareness** We have a comprehensive, recurring employee training program covering cybersecurity awareness and best practices.	
8	**Employee Behaviour Monitoring and Insider Threat Management** We monitor employee behaviour for unusual activities as part of our insider threat management program.	
9	**Software and Application Security** We maintain web application security by regularly updating and patching our software against vulnerabilities.	
10	**Physical Security of IT Assets** We ensure effective physical security measures for our IT infrastructure, including server rooms and data centres.	

Self-Assessment

Website & IT Infrastructure Security Self-Assessment

	Statements	Rating
11	**Third-Party, Vendor, and Supply Chain Security Management** We regularly conduct security assessments of third-party vendors, partners, and our supply chain to ensure they adhere to our security standards. This includes evaluating their security protocols and practices to align with our cybersecurity framework.	
12	**Hardware Redundancy and Backup Systems** We maintain backup hardware for critical components, like routers and servers, to ensure business continuity.	
13	**Backup and Data Recovery Procedures** We have robust data backup and recovery procedures, including regular backups and testing of our data recovery plan.	
14	**Security Patch Management** We have an effective process for timely application of security patches and updates to all software and systems.	
15	**Remote Access and VPN Security** We ensure secure remote access to our network through VPNs and regularly review our remote access policies.	
16	**Mobile Device and Endpoint Security** We manage and secure mobile devices and endpoints accessing our network, including implementing encryption and remote wipe capabilities.	
17	**Cloud Service and API Security** We secure our cloud services and APIs, protecting them against unauthorized access.	
18	**Internet of Things (IoT) Security** We evaluate and secure our IoT devices to protect against vulnerabilities and unauthorized access.	
19	**Compliance with Latest Security Standards** We stay updated and compliant with the latest security standards and best practices in our industry.	
20	**Regulatory Compliance and Legal Obligations** We ensure that our IT and web practices comply with all relevant regulatory requirements and legal obligations. This includes staying informed about and adhering to laws and regulations specific to our industry, region, and the types of data we handle.	

Total	