www.sansfrontiere.co.uk

Sans Frontiere Marketing Limited
73 High Street Lewes East Sussex BN7 1XG
T +44 (0) 1273 487800 F +44 (0) 1273 487811
E info@sansfrontiere.co.uk

SANS FRONTIERE SECURITY PRINCIPLES

1. Sans Frontiere Security

At Sans Frontiere we include a security hardening package with all our websites/web applications. We contract trusted third party service providers for our web hosting and, through these, we offer three levels of cloud-based hosting:

- Shared cloud hosting (this is where some server resources are shared)
- Wordpress optimized shared hosting (designed for max security and speed)
- Dedicated server hosting (designed for larger sites and high traffic demand)

Each service provider describes how their service complies with the implementation objectives and contractually commits to conform to the guidance on Cloud Security principles.

1.1. Taking payment online

We use PayPal, SagePay & WorldPay as payment gateways within our sites.

These service providers are required to comply with PCI DSS. The majority of their products form part of our PCI DSS compliance solution by so we make sure we just use and recommend these.

1.2. Our default Website Security Policy includes

• Custom firewall configuration - block fake crawlers & request throttling
• Additional login security - failed username & password lockout
• Setup non-standard webservice conventions within application
• Protect sensitive config files and core directories
• Use of proper security keys and salts
• Enforced strong password policy

1.3. Our Pro security package includes but is not limited to:

• Real-time alerts for logins, changes or suspicious activity
• Weekly monitoring for upgrades
• Core upgrades
• Plug-in upgrades
• Daily backups
• Disaster recovery (provided from a backup when a website is deemed beyond repair after a malicious attack)

2. Our actions in relation to the government security principles:

2.1. Data in transit protection
Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.

Sensitive consumer information is transmitted via an SSL connection, usually provided as part of a payment gateway service.

2.2. Asset protection and resilience
Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

These things are protected by a combination of the hosting providers server based security policy and our custom application level security policy.

2.3. Separation between consumers
Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.

This rule applies to hosting multiple websites/applications and is imposed as a rule by the hosting services we use.

2.4. Governance framework
The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

We (and our clients) inherit this aspect from the policy & SLA of our provider(s).

2.5. Operational security
The service provider should have processes and procedures in place to ensure the operational security of the service.

This is provided by a combination of the hosting providers server based security policy and our custom application level security policy.

2.6. Secure consumer management
Consumers should be provided with the tools required to help them securely manage their service.

These are usually always web based tools where web applications are concerned but we can also provide desktop / phone tools to compliment these. The later are inherently less secure however and should only be considered where they deemed essential.

2.7. Personnel security
Service provider staff should be subject to personnel security screening and security education for their role.

This is done by a combination of the hosting provider policies and our own policy.

2.8. Secure development
Services should be designed and developed to identify and mitigate threats to their security.

We strive to implement the most up-to-date security hardening and monitoring methods at the application level (see our 2 tier security policies below).

2.9. Supply chain security
The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

We use specialist security tools to audit the 3rd party tools/technologies that we use as part of our solution(s).

2.10. Identity and authentication
Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.

We develop bespoke User Access Management to meet each clients needs.

2.11. External interface protection
All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.

We implement standard security models to protect access to services via external interfaces.

2.12. Secure service administration
The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

Our administrative access is usually protected by multi layer security (ie. Access to our providers services first followed by access to our own services within the providers services) but we also implement strict security hardening principles for any exposed web based administrative portals.

2.13. Audit information provision to consumers
Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.

Our Pro security policy includes comprehensive auditing and notifications – these can be segmented into admin reports/notifications and consumer reports/notifications.

2.14. Secure use of the service by the consumer
Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

Our security hardening policy will impose these responsibilities on end users.