FyfeWeb
Hosting Services

Hosting delivered with passion and expertise

Introducing a service-focussed
Cloud hosting **partner**

Security & Responsible Disclosure Policy

support@fyfeweb.com
www.fyfeweb.com

FyfeWeb
Hosting Services

SYNOPSIS

We recognise that our Customers' information must be well managed, controlled and protected. To that end, We have a team that oversees FyfeWeb's information security program, which encompasses high-quality network security, application security, identity & access controls, change management & control, vulnerability management, third-party penetration testing, log & event management, vendor risk management, physical security, endpoint security, physical security, governance & compliance, HR & Personnel security, disaster recovery and a host of additional controls.

Our infrastructure is protected by many mechanisms and controls, including firewalls and access control, with measures implemented and scans performed regularly in order to detect or ensure that any exposed vulnerabilities are quickly found and patched.

Customer data is processed at locations throughout the UK, access to systems is restricted to specific individuals based on "need to know" principles and monitored and audited for compliance. We use Transport Layer Security (TLS) encryption (also known as HTTPS) on all websites, for all customer data transfers, and customers can elect to have all their data encrypted at rest. Our Services are solely hosted and managed in-house, and data centres we use are independently audited to ISO 9001 & ISO 27001 and Tier III (3) Standards. To ensure that we maintain the highest possible levels of information security, FyfeWeb internally conform to ISO 27001 & ISO 9001 and has procured auditing solutions from reputable third-party auditors, whom audit our information security practices annually under the UK Government Cyber Essentials standards.

If you are a customer we ask that you ensure that your appointed system administrators ensure sound security practices in maintaining access credentials to your instance of the Solutions, including strong account passwords and access restrictions to your accounts to authorised persons. Where customers become aware of a compromise to any of their account credentials, we ask that you notify us immediately by contacting our Support Team.

Security is our top priority in everything that we do as a business. This Security & Responsible Disclosure Policy outlines how anyone, usually security experts and researchers, can report vulnerabilities to the FyfeWeb Security Team in an ethical and responsible manner. We welcome researchers and experts to responsibly report any issues or lapses within our security features or mechanisms that they may come across.

We are interested in all security issues and vulnerabilities, but we are particularly interested in hearing about vulnerabilities that impact the confidentiality, availability or integrity of our systems (or our customer systems) or the information stored on these systems.

FyfeWeb
Hosting Services

1.0 - DISCLOSURE

When disclosing any security vulnerability, it must be reported to ourselves immediately via emailing our team at support@fyfeweb.com or by calling us on 0330 229 1659 providing us with clear and full details of the issue or vulnerability, and tell us precisely how You found it in order for us to reproduce the conditions, verify and validate the flaw. Should the confidentiality of any reported issues or vulnerabilities be violated (i.e. disclosure occurs to anyone who are not authorised members of the FyfeWeb Security Operations Centre) or if responsible or ethical reporting practises are not followed, it will leave you liable to civil and/or criminal liability.

In some cases, we may ask to meet with you to discuss the report at-hand. We take security extremely seriously and will respond as quickly as we can to any security issues identified. Please understand that some of our infrastructure is very complex and may take a little time to update and patch. We will respect a finder's work if the guidelines in this agreement are adhered to and we will do our best to acknowledge your disclosures and assign the necessary resources to investigate and fix potential problems as quickly as we can.

2.0 – SCANNING AND PENETRATION TESTING

Unless you have the advanced, explicit permission from the FyfeWeb Security Operations Centre (SOC), You are not permitted to conduct any form of scanning or penetration testing of any kind against any assets on and including our IP estate, network or server infrastructure without written director-level permission. If you undertake any activities without this permission will leave you wholly liable to civil and/or criminal liability or action.

3.0 – REASONABLE PERIOD

After reporting any issue or vulnerability to us, the reporting party and FyfeWeb shall agree upon a reasonable amount of time for us to address any issues before publicly disclosing such information. The default amount of time is 90 days from the notification sent by FyfeWeb to You, acknowledging receipt of your issue. However, it is worth noting that this may be extended at any point by the Company until we are satisfied that any abnormalities or vulnerabilities are fully remediated. Please note and be sympathetic that sometimes, it may be that a vulnerability resides on customer infrastructure, which we do not have access to. Should a vulnerability come to our attention that belongs to one of our customers, we will immediately notify them of any correspondence between the Company and you and advise you to contact the Customer directly – if practicable.

4.0 – UNACCEPTABLE PRACTICES

We condemn security researching activities or techniques which:

(a) Interrupts, poses a risk to or has the potential to disrupt the availability of Services to Customers
(b) That may put our or our Customer's infrastructure at further risk
(c) Using a vulnerability to carry out further activities than is necessary to establish its existence (i.e. accessing, uploading or downloading data and information) or modifying, deleting or copying information.
(d) Are brute force attacks to gain access to a system. This is not a vulnerability in the strict sense, but rather repeatedly trying passwords.
(e) Requests for remuneration for the reporting of security issues to FyfeWeb Ltd. FyfeWeb does not

operate a bug bounty programme and does not offer compensation for any vulnerabilities that are reported unless otherwise at our sole discretion of the directors. If these guidelines are followed, the security researcher will be credited on a press-release or post-mortem.

6.0 – PROMISE

Our promise to anyone reporting security vulnerabilities, we will not take legal action against those that identify security vulnerabilities, if the ethical, private reporting practices outlined in this policy are followed and adhered to and that they also adhere to international law, so please don't be hesitant or afraid to get in touch.

FyfeWeb
Hosting Services

PUBLIC DOCUMENT CONTROL

DOCUMENT TITLE:	SECURITY & RESPONSIBLE DISCLOSURE POLICY
DOCUMENT CLASSIFICATION:	NOT PROTECTIVELY MARKED
DOCUMENT OWNER	LEGAL & COMPLIANCE DIRECTORATE
DOCUMENT VERSION:	3.5
CREATION DATE:	2018-10-01
LAST REVISION:	2022-08-15
REVIEW DATE:	2023-08-15

support@fyfeweb.com
www.fyfeweb.com