FyfeWeb
The Hosting Partner of Choice

Security & Responsible Disclosure Policy

FyfeWeb
The Hosting Partner of Choice

1. We recognise that all information we manage or process must be well managed, controlled and protected. To that end, we have a team that oversees FyfeWeb's security operations, which encompasses high-quality network security, application security, identity & access controls, change management & control, vulnerability management, third-party penetration testing, log & event management, vendor & supply chain risk management, endpoint security, physical security, governance & compliance, HR & personnel security, disaster recovery and much more.

2. Infrastructure is protected by many mechanisms and controls, including firewalls and access control, with measures implemented and maintained. Infrastructure is also designed in accordance with Defence in Depth principles.

3. We regularly perform scans, audits and tests in order to detect, prevent and manage vulnerabilities or issues. Should any be found, these are quickly identified, mitigated and resolved. However, where possible, we try and prevent them.

4. Customer data is processed at secure data centre locations across the UK. Access to any of our equipment, systems, racks, data centres et al. is restricted to a limited number of specified, vetted individuals based on stringent 'need-to-know' principles. This means that they have a genuine business requirement to be accessing equipment or facilities. Access is continually monitored and audited for compliance, and access is only granted for limited amounts of time.

5. We enforce encryption on all of our websites, web interfaces, and it used in-transit, at rest and sometimes while in use.

6. Our services are hosted and managed solely in-house, and data centres we use are independently audited, highly-secure facilities that conform to ISO 9001, ISO 27001 and (TIA-942) Tier 3 Standards. Furthermore, to ensure that we maintain the highest possible levels of security end to end, FyfeWeb also conforms to ISO 27001 & ISO 9001. We have procured auditing solutions from reputable third-party auditors, including from those whom audit our security practices annually under the UK Government Cyber Essentials standard.

7. Customers are asked to ensure that their appointed system administrators ensure good security practices in maintaining access to credentials to the Services, including strong account passwords and access restrictions to your accounts to authorised persons and the services themselves. Where customers become aware of a compromise to any of their account credentials, we ask that you notify our Security Operations Centre as soon as possible.

8. Security is of utmost priority in everything that we do as a business. This Security & Responsible Disclosure Policy outlines how anyone, typically security researchers, can report vulnerabilities to FyfeWeb 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.

FyfeWeb
The Hosting Partner of Choice

1.0 - DISCLOSURE

When disclosing any security vulnerability, it must be reported to our Cyber Security Incident Response Team (CSIRT) – which is a division of the FyfeWeb Security Operations Centre (SOC) – immediately via email at: **csirt@fyfe.tech**

Our CSIRT mailbox is capable of PGP/GPG encryption, thus the only mailbox which should be used when reporting and communicating about vulnerabilities. The public key for this mailbox is hosted on our website and a link to which, can be found in our security.txt file. We require the use of PGP/GPG encryption at all times in relation to communications regarding vulnerability disclosure.

Our SOC are also contactable by email at: **security@fyfeweb.com** or by phone, calling us on: **(+44) 330 229 1659**.

Once we have established a secure communication channel, please provide 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. If you have any issues establishing a secure communication channel, please let us know before making a disclosure.

Due to the nature of the vulnerability reporting programme, utmost confidentiality is requested at all times until we (or the affected parties) have patched the vulnerability and a reasonable amount of time thereafter. Should the confidentiality of any reported issues or vulnerabilities be violated (i.e. disclosure occurs to anyone who is not authorised to know, or someone unrelated/uninvolved in the report itself) or if responsible or ethical reporting practises are not followed, you will be liable to civil and criminal proceedings and liability.

In some cases, we may ask to meet with you, either in person or virtually, 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 locate, update and patch. We will of course 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, written permission from the FyfeWeb SOC, you are not permitted to conduct any form of scanning, assessments or penetration testing of any kind against any assets on, including but not limited to our IP Address estate, network or server infrastructure. If you undertake any activities without this permission shall leave you wholly liable to civil and criminal liability/action to the fullest extent permitted by law.

3.0 – REASONABLE PERIOD OF TIME

After reporting any issue or vulnerability to us, the reporting party and FyfeWeb shall enter into a confidentiality undertaking and then agree upon a reasonable amount of time for us to address any issues before disclosing any information.

However, it is worth noting that this period of confidentiality may be extended at any point by the Company until we are satisfied that any issues or vulnerabilities are fully remediated.

Please note and be sympathetic that sometimes it may be that an issue or vulnerability resides on customer infrastructure or is part of third-party software, which we do not have access to or control over to resolve or rectify. Should a vulnerability come to our attention that belongs to one of our customers or vendors, we will immediately notify them of any correspondence between the Company and you and may refer you to contact the party in question directly.

4.0 – UNACCEPTABLE PRACTICES & OUT OF SCOPE

We condemn security researching activities or techniques which, including without limitation:

(a) Interrupts, poses a risk to, has the potential to disrupt, or otherwise impact the confidentiality, integrity or availability of systems, services, networks, accounts et al. operated by or under the control of FyfeWeb or its users and customers.

(b) Puts our data, equipment, staff, customers or infrastructure, or that of our Customer's at undue risk or load

(c) Physical security

(d) Brute forcing

(e) Social engineering

(f) Utilise a vulnerability to carry out further activities than is necessary to establish a vulnerability's existence (i.e. accessing servers, uploading or downloading data/files/information or modifying, deleting or copying information, and the like).

(g) Requests for remuneration for the reporting of security issues to FyfeWeb. FyfeWeb does not operate a bug bounty/remuneration programme and does not tend to offer compensation for any vulnerabilities that are reported, unless otherwise at the sole discretion of the directors. If these guidelines are followed, the security researcher will be credited on a post-mortem.

6.0 – PROCESS AND PROCEDURE COMPLIANCE

We promise that anyone reporting security vulnerabilities will not have legal action taken against them, when identifying and reporting security vulnerabilities, provided the ethical, private reporting practices, and guidelines outlined in this policy are followed and adhered to in full. It is also a requirement that they also adhere to the laws of England and Wales, in addition to international law, so please don't be hesitant or afraid to get in touch.

FyfeWeb
The Hosting Partner of Choice

PUBLIC DOCUMENT CONTROL

DOCUMENT TITLE:	SECURITY & RESPONSIBLE DISCLOSURE POLICY
DOCUMENT CLASSIFICATION:	NOT PROTECTIVELY MARKED
DOCUMENT OWNER	OPERATIONS DIRECTOR
DOCUMENT VERSION:	4.0
CREATION DATE:	2018-10-01
LAST REVISION:	2024-08-11
REVIEW DATE:	2025-08-11