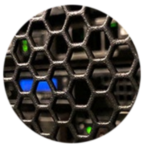
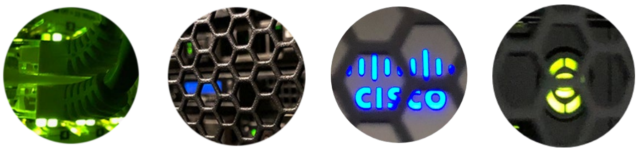


FyfeWeb
Hosting Services

Hosting delivered with passion and expertise

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

Security & Responsible Disclosure Policy



SYNOPSIS

We recognise that our all information we manage and 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 a host of additional measures and controls.

Infrastructure is protected by many mechanisms and controls, including firewalls and access control, with measures implemented and maintained. We also perform scans regularly in order to detect or ensure that any vulnerabilities or abnormalities are quickly found and resolved.

Customer data is processed at locations throughout the UK. Access to any of our systems is restricted to specific individuals based on stringent "need to know" principles and is monitored and audited for compliance.

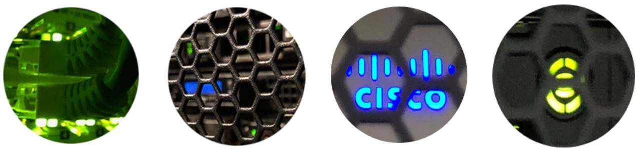
We use encryption on all websites, for all data transfers, and customers can elect to have their data encrypted at rest, either by us or by themselves.

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

If you are a customer, we ask that you ensure that your appointed system administrators ensure sound security practices in maintaining access credentials to the Services, 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 Security Operations Centre.

Security is our 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 the FyfeWeb Security Operations Centre 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 that of our customer systems) or the information stored on these systems.



1.0 - DISCLOSURE

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

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

Only 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 the location of which, can be found in our security.txt file. We require the use of PGP/GPG encryption at all times in relation to the vulnerability disclosure process.

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.

Due to the nature of the vulnerability reporting programme, utmost confidentiality is requested at all times. 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

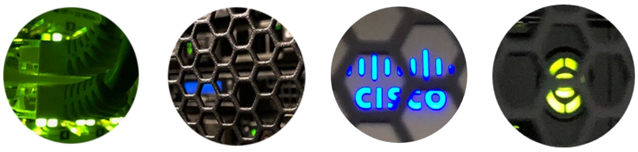
Unless you have the advanced, explicit permission from the FyfeWeb SOC, you are not permitted to conduct any form of scanning or penetration testing of any kind against any assets on, including but not limited to our IP estate, network or server infrastructure without written director-level permission.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

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 shall agree upon a reasonable amount of time for us to address any issues before disclosing any information.

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 or third-party software, which we do not have access to or control over to resolve. 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 refer you to contact the party in question directly – if practicable.

4.0 – UNACCEPTABLE PRACTICES / OUT OF SCOPE

We condemn security researching activities or techniques which:

(a) Interrupts, poses a risk to or has the potential to disrupt the availability of systems or services etc to Customers
(b) Puts our data, equipment, staff, customers or infrastructure, or that of our Customer's at undue risk
(c) Physical security, brute forcing or social engineering
(d) Using a vulnerability to carry out further activities than is necessary to establish its existence (i.e. accessing, uploading or downloading data/information or modifying, deleting or copying information and the like)..
(e) Requests for remuneration for the reporting of security issues to FyfeWeb. FyfeWeb does not operate a bug bounty programme and does not tend to 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 post-mortem.

6.0 – PROCESS AND PROCEDURE COMPLIANCE

We make a 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:	3.7
CREATION DATE:	2018-10-01
LAST REVISION:	2023-08-31
REVIEW DATE:	2024-08-15