safedrop web forms service definition

“The user's going to pick dancing pigs over security every time.” — Bruce Schneier

safedrop safedrop is a trading name of Od Consultancy Ltd.
Innovation House, Discovery Park, Sandwich, CT13 9FF **T** 00 44 20 7739 4252 angusbradley@projectfusion.com

Service Definition

Core features

Summary

Safedrop Secure Web Forms lets public sector teams create and publish secure online forms to collect sensitive information and files from external users (citizens, patients, suppliers, partners) with end-to-end encryption. Submissions are protected in transit and at rest, with access controls, audit logging, and UK data residency to support governance and compliance needs.

Who it's for

- Local authorities (revenues & benefits, housing, social care, licensing, safeguarding)
- NHS and health and care providers (referrals, patient onboarding, DSAR, complaints)
- Police and justice teams (evidence intake, statements, disclosure bundles)
- Central government and agencies (casework, procurement, whistleblowing)
- Education and public bodies (HR, admissions, sensitive reporting)

What it does

- Create secure forms with configurable fields and file upload
- Publish forms via a shareable link (public) or embed into your website
- Receive structured data and uploaded documents securely
- Route submissions to the right internal team and keep an audit trail
- Download, review, and manage submissions in a secure workspace

Secure file sharing made simple

Key benefits

- Protects sensitive submissions with end-to-end encryption
- Reduces risk compared to email attachments and consumer file-sharing
- Improves citizen/patient experience with simple, mobile-friendly intake
- Supports governance with access controls, audit logs, and retention options
- Speeds up casework by standardising intake and reducing rework

Uptime and responsiveness

• The Services shall maintain a 99.99% uptime

• The Services html pages for viewing lists of files shall load in < 5 seconds on a UK based broadband connection.

• Downloading a file shall commence within 5 seconds of clicking the download button

Supported Browsers:

- Microsoft Edge Latest two versions
- • Mozilla Firefox Latest two versions
- • Apple Safari Latest two versions
- • Google Chrome Latest two versions

Key Benefits

- **True Zero Trust design:** Every file and message is encrypted client-side
- **Sovereign UK hosting:** All data, metadata, and backups remain within UK jurisdiction.
- **Built for secure collaboration:** Ideal for councils, NHS, law enforcement, and government contractors.
- **Audit-ready:** Full logs, traceability, and role-based access control built in.

at a glance

the business

- safedrop & projectfusion are trading names of OD Consultancy Ltd, a UK company with company number 3389226.
- ISO27001 accredited company, regularly audited by UK Government approved (UKAS) auditor.
- GDPR compliant service and contracts.
- UK owned, hosted and managed. Data protected from foreign government access.
- 24x7 support (with 15 minute response 9am-530pm)
- all staff security checked to BS7858

key security measures

- data encrypted end to end
- aggressive default expiry dates and self destruct minimise data aggregation risk and attack window (e.g. with 7 day expiry if you send 10,000 drops a year only approximately 190 are available at any time)
- Detailed tamperproof logging of all activities, including command line server activity.

ISO27001:2013

"If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees." — Kahlil Gibran

We are accredited by a UKAS registered certification authority. Our Scope Statement is below. To request a copy of our ISO27001 Certificate please go to https://www.projectfusion.com/resources/ . To see our Statement of Applicability or other security documents please email support@projectfusion.com

Scope Statement

The scope of the OD Consultancy Ltd ISMS is:

"The provision of Secure Hosting for customer data through a number of 'Software as a Service' products. The Information Security Management System includes all Information and Information Processing equipment owned by, or in the custody of the company; all people employed by OD Consultancy Ltd, including contractors; all business functions and processes, including the management and configuration of software, testing processes and procedures, protection and integrity of code and libraries, and physical/procedural/personal security of the coding environment."

GDPR

Safedrop/PROJECTFUSION offers a secure Content Management System with features to help you meet your global compliance obligations. We are fully GDPR compliant.

For customers subject to GDPR we can keep all data in the UK at all times. We can also offer a unique online editor, that lets users view & work with Microsoft Office documents online, but not download them.

We can provide numerous privacy related tools to help you including:

Personal trashcans with automated deletion, encryption at rest and in transit, setting time based alerts on files, automated business rules to apply metadata and tags to content on upload, standards based export tools to export huge datasets, and a very fast search.

For a GDPR checklist and to request a GDRP addendum to an existing contract please visit https://www.projectfusion.com/resources/

safedrop features for safedrop official

“If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.” — Kahlil Gibran

restricted subdomain* - especially useful with good firewalls!

The application runs in it’s own subdomain for your organisation. For maximum security, if you use application level firewalls you can setup your own safedrop domain - e.g. https://acme.safedrop.com , and restrict your firewall to allow access to this domain only. This prevents insider use of generic safedrop to send files out, useful as SSH transmissions can otherwise not be logged. *Cost option

read receipts and audit trail by email

safedrop senders will receive an email delivery receipt and audit trail of all activity for each drop, including SHA checksums, IP Address and times. So in years to come, you have proof of delivery and download, right there in your email.

manage users

Admins can add and remove users in seconds. Admins can setup rules to monitor content of safedrops.

When users lose access to their email address (e.g. on leaving your business) they automatically lose access to their sent drops.

online searchable audit trail

All transmissions are logged for security purposes. All file deliveries and recipients are stored in a database accessible by system administrators. safedrop administrators can access audit trails for *all* safedrops sent by their organisation, and free text search against these drops, or search for drops by a particular user.

awesome easy API

Easy API means you can easily integrate safedrop.

people and process security

You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable. — Daryl White, DOI CIO

All employees trained on information security and privacy procedures

All employees trained on information security and privacy procedure. An expert 4 man 3rd line support team, under strict NDA, are the only people with access to your server. Written permission is required before our support team will view or examine any files in your **safedrop** instance. New starts are identity checked to BS7858 level, and employed for at least 2 months before being given access to servers.

Any handling of client data is ruled by our ISO27001 compliant information labelling and handling procedure which includes steps like only downloading client data to funky FIPS 140-2 Level 3 usb drives.

We like security!

We hire people who are interested in security, and in making things better. We spend a lot of time thinking about how to make security simple.

Regular risk assessments

We undertake quarterly risk analysis and evaluation on all our assets in line with the requirements of ISO/IEC 27001.

infrastructure security

The mantra of any good security engineer is: 'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together. — Bruce Schneier

All data stored iUK Data Centres (as specified)

All servers are hosted in ISO 27001 audited data centres, with our ISO27001 accredited partners.These partners maintain network security & intrusion detection systems.
Hosting personnel do not have terminal level access to safedrop servers operating systems or file storage. All data and backups kept in the UK at all times.

3rd Party Audits

Servers & application are regularly scanned, penetration tested and security checked.

Physical Security

All information is stored in servers housed in enterprise-level secure facilities. Strictly monitored access to all data centre using keycard protocols, biometric scanning protocols and continuous interior and exterior surveillance. Access limited to data centre personnel only without exception. All data centre employees undergo thorough background security checks before being employed. All servers use Raid 6 disk storage and are backed up daily, with all data encrypted offsite.

Conditioned Power

Power systems in our data centres are designed to run uninterrupted even in the unlikely event of a total power outage. All servers are fed with conditioned UPS (Uninterruptible Power Supply) power that will run if utility power fails.

Data destruction

A potential threat to data security is recycling of hardware back into our pool. Our approach to this is two-fold.

First, whenever a server which has contained customer data is de-provisioned its hard disks are labelled as "DIRTY" in our asset management system. Our automated systems will not allow such a hard drive to be redeployed until it has been "cleaned" which we do by overwriting the entire disk with random data twice.

For purists, yes if data is only overwritten twice it is theoretically possible to examine the hard drive under a scanning electron microscope looking at the edges of the tracks and determine the previous binary state with sufficient accuracy to reconstitute the data (at staggering expense, it should be noted). However, all the hardware remains in our control, in our secure data centres,

and access only by our authorised personnel. Two wipes is sufficient to prevent data recovery via the hard disks own mechanisms.

At end of life the the disks and their magnetic platters are shredded - reduced to small fragments, from which data recovery would be impossible.