Frabs

LEGAL · VERSION 5

Terms and Conditions

The agreement between Frabs and the businesses that use Frabs Server, Frabs Host and Frabs Hypervisor, including data processing, sub-processors and security.

VERSION	APPLIES TO	GOVERNING LAW	CONTACT
FRABS_TC_V.5 OCTOBER 2026	The free Trial and every paid subscription	England and Wales	frabs.net info@frabs.net

Contents

1.	DEFINITIONS	4
2.	STRUCTURE OF THE AGREEMENT	6
3.	THE SERVICE	6
4.	ACCOUNTS AND ACCESS	7
5.	FREE TRIAL	7
6.	LICENSES AND FEES	8
7.	PAYMENT AND TAXES	9
8.	CUSTOMER RESPONSIBILITIES	9
9.	ACCEPTABLE USE	10
10.	DETECTION, ATTRIBUTION AND REMEDIATION	10
11.	DATA PROTECTION	11
12.	SECURITY	11
13.	SUPPORT	11
14.	AVAILABILITY AND MAINTENANCE	12
15.	SUSPENSION	12
16.	INTELLECTUAL PROPERTY	13
17.	CONFIDENTIALITY	13
18.	WARRANTIES	14
19.	INDEMNIFICATION	14
20.	LIMITATION OF LIABILITY	15
21.	TERM AND TERMINATION	16
22.	CHANGES	16
23.	NOTICES AND COMMUNICATIONS	17
24.	GENERAL	17
Schedule A	FEES	19
Schedule B	SUPPORT	20
Schedule C	DATA PROCESSING	20
Schedule D	SUB-PROCESSORS AND SERVICE PROVIDERS	22
Schedule E	SECURITY MEASURES	23

About these Terms. These Terms are between Frabs and the business that creates an Account or signs an Order. They apply to the free Trial and to every paid subscription. By accepting them when registering at

frabs.net, in the Panel, or by signing an Order, the Customer agrees to them. Words that start with a capital letter are defined in clause 1.

1. DEFINITIONS

1.1 In these Terms, the words below have the meanings given to them. A defined term has the same meaning in the singular and in the plural.

Account	the Customer's account with Frabs, which holds its Licenses, Authorised Users, billing details, Tickets, settings, Incidents and audit log.
Affiliate	a company that controls, is controlled by, or is under common control with a party.
Agreement	the contract between Frabs and the Customer made up of the documents listed in clause 2.1.
Approval	a decision by an Authorised User, made in the Panel, that allows Frabs to carry out a Remediation Action.
Authorised User	a person the Customer has invited to its Account, with the role of owner, admin, analyst or a read-only role.
Business Day	a day other than a Saturday, a Sunday or a public holiday in England.
Business Hours	the hours that fall within Support Hours.
Confidential Information	information that is marked as confidential or that a reasonable person would understand to be confidential, including the Customer Data, the Documentation, pricing agreed in an Order and the non-public workings of the Service.
Custom Domain	an address on a domain that the Customer controls, such as frabs.example.com, at which the Panel is made available under clause 4.7.
Customer	the business that creates an Account or signs an Order.
Customer Data	all data that the Customer or its Authorised Users put into the Service, and all data collected about the Customer's Protected Servers and networks by the Sensor, including Detection Data.
Customer Personal Data	Personal Data that is part of the Customer Data and that Frabs processes as processor for the Customer.
Data Protection Law	the UK GDPR, the Data Protection Act 2018 and, where it applies, Regulation (EU) 2016/679, each as amended or replaced.
Detection Data	network flow metadata and abuse indicators that the Sensor collects and the Service analyses, such as source and destination addresses, ports, protocols, volumes and timings, the attribution of activity to a Protected Server or a Workload, and readings of the computing resources that a Protected Server and its Workloads use, such as CPU, disk and memory.
Documentation	the guides, install instructions and help pages that Frabs publishes for the Service.
End Customer	a person or business that rents or uses a Workload, or another service, from the Customer.
Fees	the amounts payable for the Service, as set out in clause 6, Schedule A and any Order.
Frabs	the business that operates the website frabs.net and provides the Service.

Incident	a pattern of activity, inbound or outbound, that the Service has detected and attributed to a Protected Server, a Workload or an End Customer, and the record of how it was handled.
License	the right to run the Sensor on one Protected Server for one Product.
Order	an order form, quote or online checkout, including registration at frabs.net, in which the Customer subscribes to the Service, whether or not it is signed.
Panel	the Frabs control panel at panel.frabs.net or at a Custom Domain, the Customer's account pages at frabs.net, and the Frabs API at api.frabs.net.
Personal Data	has the meaning given in Data Protection Law.
Product	Frabs Server, Frabs Host or Frabs Hypervisor, as described in clause 3.2.
Protected Server	one physical dedicated or bare-metal server on which the Sensor is installed under a License: a standalone server for Frabs Server, a hosting server for Frabs Host, or a virtualisation host for Frabs Hypervisor.
Remediation Action	a step that limits or stops an attack, abuse or resource abuse, such as rate limiting, blocking traffic, isolating a Workload from the network, limiting the CPU or disk that a Workload uses, or notifying an End Customer.
Sensor	the Frabs software that runs on a Protected Server and observes the traffic to and from it and its Workloads, and the computing resources they use. On a virtualisation host it runs at the hypervisor level. No Frabs software is installed inside an End Customer's virtual server.
Service	the Frabs network protection and server monitoring service, in each of its Products, made up of the Sensor, the Panel, the Frabs API, and the support provided under clause 13.
Stripe	Stripe, the payment processor that Frabs uses to take payments, as listed in Schedule D.
Sub-processor	a third party that Frabs engages to process Customer Personal Data.
Subscription Term	the period during which the Customer has a paid subscription to the Service, as described in clause 21.
Support Hours	09:00 to 18:00 UK time on Business Days.
Terms	these Frabs Terms and Conditions, including their Schedules.
Ticket	a support request that an Authorised User raises in the Panel.
Tier	the price band that applies to the Licenses of one Product, set by the number of Licenses of that Product the Customer holds, as listed in Schedule A.
Trial	the free trial described in clause 5.
Trial Period	the 30 days that start when the Trial begins under clause 5.
Workload	a virtual server, container, hosting account, website, game server or other service that runs on a Protected Server, whether for the Customer or for an End Customer.

1.2 A reference to a clause or Schedule is to a clause of, or a Schedule to, these Terms. Headings are for convenience only. The words "including" and "for example" do not limit the words before them.

2. STRUCTURE OF THE AGREEMENT

2.1 The Agreement is made up of the following documents. If they conflict, the document that is higher in this list prevails, except that Schedule C prevails over the rest of these Terms on the processing of Customer Personal Data.

(a) the Order, but only for the Licenses, Fees and any special terms it states;

(b) these Terms, including Schedule A (Fees), Schedule B (Support), Schedule C (Data processing), Schedule D (Sub-processors and service providers) and Schedule E (Security measures); and

(c) the Documentation.

2.2 These Terms apply to every Order. Terms that the Customer proposes, including terms on a purchase order or in a supplier portal, do not apply, even if Frabs does not object to them.

2.3 The Service is for businesses. The Customer confirms that it uses the Service only for the purposes of its business and not as a consumer.

2.4 The Agreement starts when the Customer accepts these Terms when it registers at frabs.net, accepts them in the Panel or signs an Order, whichever happens first. The person who accepts confirms that they have authority to bind the Customer.

3. THE SERVICE

3.1 Frabs provides the Service to the Customer under the Agreement. The Service helps the Customer to protect its Protected Servers and its network, and to prevent abuse that comes from them, in these steps:

(a) detect: the Sensor observes traffic to and from the Customer's Protected Servers and the resources that they and their Workloads use, and the Service identifies attacks and patterns of abuse;

(b) attribute: the Service links the activity to a Protected Server or a Workload and, where the information is available, to an End Customer;

(c) investigate: the Service gives Authorised Users the evidence they need to review the Incident in the Panel;

(d) remediate: Remediation Actions are carried out as set out in clause 10; and

(e) record: the Service keeps a record of each Incident, each decision and each action in an audit log.

3.2 The Service is offered as three Products, each sold by the License:

(a) Frabs Server, for standalone Linux servers;

(b) Frabs Host, for website, reseller and game hosting servers. The Service attributes activity to hosting accounts or domains to the extent that the Customer's hosting panel integration provides that information; and

(c) Frabs Hypervisor, for virtualisation hosts. The Sensor works at the hypervisor level and observes each virtual server from outside it.

3.3 Frabs does not require, and the Customer must not install, any Frabs software inside an End Customer's virtual server.

3.4 Frabs may improve, update or change the Service from time to time. If a change would materially reduce what the Service does, clause 22 applies.

3.5 Frabs may use subcontractors to provide the Service and remains responsible for their work to the same extent as for its own.

3.6 The Service is a tool to help the Customer protect its systems and manage abuse. It does not replace the Customer's own security, abuse handling and legal responsibilities, and Frabs does not promise that every attack or abuse event will be detected, correctly attributed, mitigated or stopped.

4. ACCOUNTS AND ACCESS

4.1 To use the Service the Customer must create an Account and give accurate information about itself. The Customer must keep that information up to date.

4.2 Accounts and Authorised Users must use an email address at a domain that the Customer or its business controls. Frabs may refuse personal, free or disposable email addresses.

4.3 Every Authorised User must sign in with multi-factor authentication. The Customer must ensure that each Authorised User keeps their sign-in details, authenticator app, recovery codes and sign-in codes secret and does not share them.

4.4 The Customer chooses the role of each Authorised User. Owners and admins can change settings, approve Remediation Actions and manage other users. Analysts can investigate Incidents and raise Tickets. Read-only roles can view information. Only the owner can manage billing and the Custom Domain. The Customer is responsible for deciding who gets which role.

4.5 The Customer is responsible for everything that is done in its Account, including by its Authorised Users, unless the activity was caused by Frabs failing to meet clause 12.

4.6 The Customer must tell Frabs without delay if it suspects that an Account, a sign-in credential or a Protected Server has been compromised. Frabs may require an Authorised User to confirm their identity again before a sensitive action, such as changing billing details or approving a Remediation Action.

4.7 Custom Domain. The Panel is available at panel.frabs.net. The Customer may instead make it available at one Custom Domain. To do so, the Customer must control the domain and publish the DNS records that the Panel shows. The Customer authorises Frabs and its service providers to check those records and to obtain and renew a TLS certificate for the Custom Domain. If the records are removed or changed, the Panel may stop being available at the Custom Domain, and remains available at panel.frabs.net. The Customer may change or remove its Custom Domain at any time, and a new Custom Domain is checked again before it is used.

5. FREE TRIAL

5.1 Frabs offers a free Trial of one License of one Product. The Trial lasts for the Trial Period. Frabs also offers a demo of the Service. The Customer is welcome to use the demo and the Trial to decide whether the Service meets its needs before it pays for the Service.

5.2 There is one Trial for each company. Frabs treats Accounts whose owners use email addresses at the same domain as the same company. A domain, or a server, that has been used for a Trial under any Account cannot be used for another Trial.

5.3 During the Trial the Customer may connect one Protected Server only. The Trial has every feature of the Product.

5.4 Frabs may refuse or end a Trial if it reasonably believes that the Customer is trying to get more than one Trial for the same company or server, for example by creating several Accounts.

5.5 To start the Trial the Customer must set up a payment method with Stripe when it registers. No Fees are charged during the Trial Period.

5.6 The Trial continues into a paid subscription for one License of the chosen Product, at that Product's Fee for one License, unless the Customer cancels before the Trial Period ends. If the Customer has not cancelled in its Account by the end of the Trial Period, Frabs will charge the first monthly Fee to the Customer's payment method, and the subscription continues as set out in clause 21. Frabs will send a reminder by email before the Trial Period ends, but the Customer is responsible for cancelling in time.

5.7 If the Customer cancels before the Trial Period ends, no Fees are charged and the Service stops at the end of the Trial Period. Frabs will keep the Customer's Account data for 30 days after that, in case the Customer decides to subscribe, and will then delete it.

5.8 The Service is provided during the Trial on an "as is" basis, without any service targets. Clauses 18 and 20 apply to the Trial, and Frabs's liability for the Trial is as set out in clause 20.6.

6. LICENSES AND FEES

6.1 The Fees are charged for each License, by Product, at the rates set out in Schedule A. Every License of a Product is charged at the rate of the Tier that matches the total number of Licenses of that Product that the Customer holds, subject to that Tier's monthly minimum.

6.2 The Tier for each Product follows the number of Licenses of that Product automatically. The Customer does not need to choose or change a Tier.

6.3 The Customer may add Licenses at any time in its Account. Nothing is charged when a License is added. The next invoice covers the added License for the rest of the billing month in which it was added, and the billing month ahead at the Tier that then applies.

6.4 When the Customer reduces its Licenses, the Fees change from the start of the next billing month. Fees already paid for the current billing month are not refunded, as set out in clause 7.

6.5 Partner programme. While the Customer is approved under the Frabs partner programme and shows the Frabs badge on its website as Frabs requires, the Fees for its Frabs Host and Frabs Hypervisor Licenses are reduced by the percentage that Frabs publishes for the programme, which is 25% at the date of these Terms. The discount does not apply to Frabs Server Licenses. If the badge is removed, Frabs may end the discount from the start of the next billing month.

6.6 Fees for any other discount or special terms agreed with Frabs, such as reseller pricing, are set out in the Order or in a separate written agreement.

6.7 Frabs may change its Fees by giving the Customer at least 30 days' written notice. The new Fees apply from the start of the first billing month that begins after the notice period. If the Customer does not agree to the change, it may cancel under clause 21.2 before the new Fees apply.

7. PAYMENT AND TAXES

7.1 The Service is sold as a subscription. Unless an Order says otherwise, the Customer's subscription renews automatically each month and the Fees are charged monthly in advance, using the payment method that the Customer has set up in its Account, until the subscription is cancelled under clause 21. All payments are made through Stripe, which Frabs uses as its payment processor. By setting up a payment method the Customer authorises Frabs, through Stripe, to charge the Fees to it on a recurring basis. Frabs does not store full card details, and Stripe's own terms apply to its handling of them.

7.2 Fees are shown in US dollars and do not include VAT or any other tax, duty or charge. The Customer must pay any such amounts that apply to the Service, and Frabs will add VAT to its invoices where it is required to.

7.3 Frabs will send each invoice by email to the billing contact set in the Account and will make it available in the Account.

7.4 If a payment fails, Frabs may try it again and will tell the Customer. If the Fees are still unpaid 7 days after Frabs's notice, Frabs may suspend the Service under clause 15.

7.5 If the Customer disputes an invoice in good faith, it must tell Frabs within 30 days of the invoice date, giving its reasons, and must pay the part that is not in dispute. The parties will work together to settle the dispute promptly.

7.6 Frabs may charge interest on late payments at 4% a year above the Bank of England base rate, from the due date until payment, to the extent the law allows.

7.7 Fees are not refundable. This applies to every Product and Tier and to a Trial that continues into a paid subscription, including where the Customer cancels part-way through a billing month, does not use the Service, or changes its mind. The Customer has the demo and the free Trial to try the Service before it pays. This clause does not limit a refund that the law requires or that clause 21.4 provides.

8. CUSTOMER RESPONSIBILITIES

8.1 The Customer must:

(a) install and keep up to date the Sensor on its Protected Servers in line with the Documentation;

(b) have the right to install the Sensor on each Protected Server, to monitor the traffic to and from it and its Workloads, and to monitor and limit the computing resources they use;

(c) make sure that its terms with End Customers allow the monitoring and the Remediation Actions that the Service involves, and give any notices to End Customers that the law requires;

(d) give accurate and current information that the Service needs, for example about which End Customer a Workload belongs to;

(e) review Incidents and Approval requests in good time; and

(f) comply with the law that applies to its use of the Service.

8.2 The Customer is responsible for its network, its Protected Servers, its Workloads, its End Customers and its relationships with them. Frabs has no contract with End Customers and no responsibility to them.

8.3 The Customer is responsible for dealing with attacks, abuse complaints, blocklist listings and similar matters that concern its network, even if the Service has helped to detect or reduce them.

8.4 The Customer remains responsible for the security of its Protected Servers, networks and Workloads, including firewalls, patching, backups, access control and its own incident response. The Service is in addition to those measures and does not replace them.

8.5 The Customer must give Frabs the help and information that Frabs reasonably asks for to provide the Service. Frabs is not responsible for delay or failure that the Customer causes.

9. ACCEPTABLE USE

9.1 The Customer must not, and must not allow anyone else to:

(a) use the Service in a way that breaks the law, including sanctions, export control and data protection laws;

(b) use the Service to monitor people or traffic that the Customer has no right to monitor;

(c) copy, modify, reverse engineer or try to obtain the source code of the Service, except where the law allows it despite this restriction;

(d) attack, probe, overload or interfere with the Service or its security, or try to get round its limits, including the limits of the Trial;

(e) resell the Service, or offer it to others as a service or as part of a service, without Frabs's written agreement, such as approval under the Frabs reseller programme;

(f) use the Service to build a competing product; or

(g) put into the Service anything that is unlawful or that contains malicious code.

9.2 The Customer must not use the Frabs API in a way that exceeds the rate limits in the Documentation.

9.3 If the Customer breaks this clause, Frabs may act under clause 15.

10. DETECTION, ATTRIBUTION AND REMEDIATION

10.1 The Service shows the Customer what it has detected and how confident it is. Detection is based on patterns and can be wrong. Some attacks and abuse will not be detected, and some activity that is not an attack or abuse may be flagged.

10.2 The Customer decides which Remediation Actions are available on its Account and who may approve them.

10.3 Frabs will carry out a Remediation Action only:

(a) after an Authorised User has given an Approval for that action; or

(b) under an automation rule that the Customer's owner or admin has switched on in the Panel, and only to the extent that the rule covers that action.

10.4 Where the Customer gives an Approval or switches on an automation rule, the action is taken on the Customer's instruction. The Customer is responsible for the effect of the action, including its effect on an End Customer.

10.5 The Customer may reverse a Remediation Action in the Panel, or ask Frabs to do so by raising a Ticket.

10.6 The Service records each Incident, each Approval, each automation rule and each Remediation Action in the audit log of the Account, with the time and the Authorised User or rule that was responsible.

10.7 Frabs is not liable for a Remediation Action that the Customer approved or that its own automation rule triggered, or for a detection that is wrong or that was missed, except to the extent that the problem was caused by Frabs's breach of the Agreement.

11. DATA PROTECTION

11.1 Each party must comply with Data Protection Law.

11.2 Frabs is the controller of the Personal Data of the Customer's Authorised Users that it holds in order to run Accounts, bill the Customer, keep the Service secure and communicate with the Customer. That data is described in the Frabs Privacy and Cookie Notice.

11.3 For Customer Personal Data, the Customer is the controller and Frabs is the processor, and Schedule C applies.

11.4 The Service is designed to analyse network flow metadata, abuse indicators and resource use readings, not the content of End Customer traffic, files or memory. The Customer must not use the Service to send the content of its End Customers' communications to Frabs.

11.5 Frabs may use data that has been aggregated and made anonymous so that it cannot identify the Customer, an End Customer or any person, in order to run, secure and improve the Service.

12. SECURITY

12.1 Frabs will use appropriate technical and organisational measures to protect the Customer Data, taking into account the risk and the state of the art. The measures are described in Schedule E.

12.2 Frabs personnel may look at a Customer's Account only to provide support, to keep the Service secure or as the law requires. When they do so using a view of the Customer's Account:

(a) the view is read-only;

(b) the person must record a reason for it;

(c) it lasts for no more than 30 minutes unless it is renewed with a new reason; and

(d) the access is logged and shown in the Customer's own audit log.

12.3 If Frabs becomes aware of a security breach that affects the Customer Data, it will tell the Customer as set out in Schedule C, take steps to contain it and give the Customer the information it reasonably needs.

12.4 The Customer must keep its own systems, including the Protected Servers on which the Sensor runs, reasonably secure, and must apply updates to the Sensor that Frabs identifies as security updates within a reasonable time.

13. SUPPORT

13.1 Frabs provides support for the Service through Tickets only. Support is available to the Customer's Authorised Users who are signed in to their Account with multi-factor authentication. The roles of owner, admin and analyst can raise Tickets and reply to them, and read-only roles can view them.

13.2 Frabs does not give support by telephone or through the sales chat on the Frabs website, and does not answer support questions by email. The only email exception is that a person who cannot sign in may email info@frabs.net to get access back. Otherwise, the sales chat and info@frabs.net are for questions about buying the Service and are not part of the support service. A reply to a Frabs notification email does not reach the support team.

13.3 Notification emails about a Ticket tell the Customer that there has been an update and do not contain the text of the Ticket. The Customer must sign in to read it.

13.4 Frabs will answer Tickets during Support Hours. Frabs aims to send a first reply within the target shown in Schedule B for the number of Licenses the Customer holds. These targets are aims and not guarantees, and they are counted in Business Hours within Support Hours.

13.5 Frabs sets the priority of a Ticket, taking the Customer's description into account. Frabs may use internal notes on a Ticket, which are not shown to the Customer.

13.6 A Ticket is solved when Frabs has answered it or dealt with it. A solved Ticket closes automatically after 7 days unless the Customer replies, in which case it is reopened.

13.7 The Customer should not put passwords, keys or other secrets into a Ticket. If a Ticket needs logs, the Customer should paste only the relevant lines, and Frabs may ask the Customer to send diagnostic information that the Sensor can attach.

13.8 Support does not include work on the Customer's own systems, other than helping the Customer to install and run the Sensor in line with the Documentation.

14. AVAILABILITY AND MAINTENANCE

14.1 Frabs will provide the Service with reasonable skill and care and will use reasonable efforts to keep the Panel and the Frabs API available.

14.2 Frabs will try to carry out planned maintenance outside Support Hours and will give notice of planned maintenance that is likely to affect the Service. Frabs may carry out urgent maintenance without notice if it is needed for security or to prevent damage to the Service.

14.3 The Service depends on the internet, on the Customer's DNS and on third-party services. Frabs is not responsible for failures that are outside its reasonable control.

14.4 Frabs does not promise that the Service will be uninterrupted or free of faults. If the Service fails for a long period because of Frabs's breach of the Agreement, the Customer's remedies are those set out in clause 21.3 and clause 20.

15. SUSPENSION

15.1 Frabs may suspend the Service, or part of it, immediately and without liability if:

(a) the Customer has not paid Fees that are due, as set out in clause 7.4;

(b) the Customer or an Authorised User has seriously or repeatedly broken clause 9 or clause 8;

(c) the suspension is needed to protect the security or integrity of the Service or of other customers;

(d) Frabs is required to do so by law or by a court or authority; or

(e) Frabs reasonably believes that the Account or a credential has been compromised.

15.2 Where it is reasonable and lawful to do so, Frabs will tell the Customer before suspending, or as soon as possible afterwards, and will say what the Customer must do to have the Service restored.

15.3 Frabs will restore the Service as soon as the reason for the suspension has ended. The Fees remain payable during a suspension that was caused by the Customer.

15.4 A suspension of the Service does not stop a Remediation Action that is already in place from continuing until the Customer reverses it.

16. INTELLECTUAL PROPERTY

16.1 Frabs and its licensors own all rights in the Service, the Sensor, the Panel, the Frabs API, the Documentation and the Frabs name, logo and badge. Nothing in the Agreement transfers any of those rights to the Customer.

16.2 Frabs gives the Customer a non-exclusive, non-transferable right, for the Subscription Term and the Trial Period, to use the Service and to install and run the Sensor on its Protected Servers under its Licenses, for its own internal business purposes and in line with the Agreement.

16.3 The Customer owns the Customer Data. It gives Frabs the right to use the Customer Data only to provide, secure and support the Service and as set out in clause 11 and Schedule C.

16.4 If the Customer gives Frabs feedback or suggestions about the Service, Frabs may use them without charge or restriction.

16.5 The Customer may say that it uses the Service, and a partner approved under the partner programme may show the Frabs badge as Frabs provides it. Otherwise the Customer must not use the Frabs name or logo in a way that suggests that Frabs endorses it, without Frabs's written permission.

17. CONFIDENTIALITY

17.1 Each party must keep the other's Confidential Information confidential, use it only for the Agreement and not disclose it except as set out in this clause.

17.2 A party may disclose Confidential Information to its employees, Affiliates, professional advisers and subcontractors who need to know it for the Agreement and who are bound by similar duties of confidentiality.

17.3 This clause does not apply to information that is or becomes public without a breach by the receiving party, that the receiving party already had or received lawfully from someone else, or that it develops on its own.

17.4 A party may disclose Confidential Information if the law or a court or authority requires it to, as long as it gives the other party notice first where it lawfully can.

17.5 This clause continues for 3 years after the Agreement ends, and for as long as the information remains a trade secret.

18. WARRANTIES

18.1 Each party confirms that it has the power and authority to enter into the Agreement.

18.2 Frabs confirms that it will provide the Service with reasonable skill and care and in line with the law that applies to it.

18.3 The Customer confirms that it has the rights, consents and permissions described in clause 8.1 and that the Customer Data does not break any law or any right of a third party.

18.4 Except as stated in the Agreement, Frabs gives no warranty or condition, express or implied, including about satisfactory quality, fitness for a particular purpose, accuracy, or that the Service will detect, prevent, mitigate or stop all attacks or abuse. Those warranties and conditions are excluded as far as the law allows.

18.5 The Customer acknowledges that no security, monitoring or abuse prevention service can be perfect, and that the Service is only one of the measures the Customer should use.

19. INDEMNIFICATION

19.1 The Customer will pay for and defend Frabs against any claim brought by a third party, including an End Customer, and will pay the damages that a court finally awards, or that the Customer agrees to in settlement, to the extent the claim arises from:

(a) the Customer's use of the Service in breach of clause 8 or clause 9;

(b) a Remediation Action taken on the Customer's Approval or under the Customer's automation rule, except where the claim is caused by Frabs's breach of the Agreement;

(c) the Customer Data, or the Customer's monitoring of traffic, breaking a law or a right of a third party; or

(d) an attack on, or abuse of or from, the Customer's Protected Servers, Workloads or network, except where the claim is caused by Frabs's breach of the Agreement.

19.2 Frabs will pay for and defend the Customer against any claim that the Customer's use of the Service in line with the Agreement infringes a third party's intellectual property rights, and will pay the damages that a court finally awards, or that Frabs agrees to in settlement. Frabs has no duty under this clause to the extent that the claim arises from the Customer Data, from a change made by the Customer, or from use of the Service with something that Frabs did not provide.

19.3 If a claim of this kind is made, Frabs may change the Service so that it no longer infringes, get the right for the Customer to continue to use it, or end the Agreement for the affected part.

19.4 A party that seeks protection under this clause must tell the other promptly of the claim, let it take over the defence and settlement, and give reasonable help at the other's cost. A late notice relieves the other party only to the extent that it has been harmed by the delay. Clause 19.2 and clause 19.3 are Frabs's only liability for infringement of intellectual property rights.

20. LIMITATION OF LIABILITY

20.1 Nothing in the Agreement limits or excludes a party's liability for death or personal injury caused by its negligence, for fraud or fraudulent misrepresentation, or for any other liability that cannot be limited or excluded by law. Every other part of this clause is subject to this clause 20.1.

20.2 Frabs is not liable to the Customer, whether in contract, tort (including negligence), breach of statutory duty or otherwise, for:

(a) loss of profit, revenue, business, contracts, customers, goodwill or anticipated savings;

(b) loss or corruption of data, except as set out in clause 20.5;

(c) any indirect or consequential loss;

(d) any loss that arises from an attack on, an intrusion into, or abuse of or from the Customer's Protected Servers, Workloads, networks or End Customers, as set out in clause 20.3;

(e) a detection that is wrong or that was missed, or a Remediation Action that the Customer approved or that its own automation rule triggered;

(f) the Service, the Panel, a Custom Domain or the Frabs API being unavailable, slow or faulty, or the Sensor stopping or failing to act;

(g) the Customer's DNS, hosting provider, upstream providers, integrations, payment provider or any other third party, or anything outside Frabs's reasonable control; or

(h) any claim by an End Customer or other third party against the Customer,

whether or not the loss could have been foreseen, and whether or not Frabs was told that it might happen.

20.3 Attacks on the Customer's systems. The Service is designed to reduce, not remove, the risk of attacks and abuse. Frabs is not liable for any loss, damage, downtime, loss of data, cost or claim that arises from an attack on, an intrusion into, or abuse of or from the Customer's Protected Servers, Workloads, networks or End Customers, including a denial-of-service attack, a scan, the compromise of a server or account, malware, spam or resource abuse, whether or not the Service detected, reported or acted on it. This includes loss caused by an attack that the Service did not detect or did not stop in time, and the cost of the Customer's own response and recovery and of its dealings with its End Customers, upstream providers and blocklists.

20.4 Frabs's total liability to the Customer under or in connection with the Agreement, for all claims together, is limited to the Fees that the Customer paid for the Service in the 3 months before the event that gave rise to the first claim.

20.5 Frabs's liability for the loss or corruption of Customer Data is limited to using reasonable efforts to restore it from the latest backup, and counts toward the limit in clause 20.4.

20.6 During the Trial the Service is free, and Frabs has no liability to the Customer for the Trial except a liability that cannot be excluded under clause 20.1.

20.7 The Customer's duty to pay the Fees, and its liability under clause 19.1 or for a breach of clause 9, are not limited by this clause.

20.8 The Customer must bring any claim against Frabs within 6 months after it became aware, or should reasonably have become aware, of the event that led to it, or the claim is barred.

20.9 The parties are businesses, and the Customer has had the chance to try the Service free of charge before paying. The parties agree that the exclusions and limits in this clause are reasonable, taking into account the Fees, the nature of the Service, the free Trial and demo, and the fact that the Customer controls its own systems and End Customers. If any exclusion or limit is found to be unenforceable, the rest of this clause continues to apply, and Frabs's liability is limited to the smallest amount that the law allows.

21. TERM AND TERMINATION

21.1 The Agreement starts as set out in clause 2.4. The Subscription Term begins when the Customer's first paid billing month starts, including when the Trial continues into a paid subscription under clause 5.6. It renews automatically each month until it is ended under this clause.

21.2 The Customer may cancel its subscription at any time in its Account, including during the Trial Period. A cancellation during the Trial Period takes effect as set out in clause 5.7. Any other cancellation takes effect at the end of the current billing month, and the Service continues until then. Fees that have been paid are not refunded, as set out in clause 7.7.

21.3 Either party may end the Agreement immediately by written notice if the other:

(a) commits a material breach that cannot be put right, or that it does not put right within 14 days after notice asking it to do so;

(b) becomes insolvent, enters administration, liquidation or a similar process, or stops carrying on business; or

(c) is no longer able to carry out its duties because of an event described in clause 24.4 that lasts for more than 60 days.

21.4 Frabs may also end the Agreement for any reason by giving the Customer at least 60 days' written notice. In that case Frabs will refund any Fees paid for the period after the end of the Agreement.

21.5 When the Agreement ends:

(a) the Customer's right to use the Service ends, and the Customer must remove the Sensor from its Protected Servers;

(b) the Customer must pay all Fees that have fallen due; and

(c) any Remediation Action that is still in place stays in place until the Customer reverses it.

21.6 The Customer may export its Incident records and audit log from the Panel at any time until the Agreement ends, and for 30 days after it. Frabs will help with that if the Customer raises a Ticket within those 30 days.

21.7 Frabs will delete the Customer Data within 30 days after the end of that export period, unless the law requires Frabs to keep some of it. Backup copies are deleted in line with Frabs's normal backup cycle. Frabs will confirm the deletion if the Customer asks.

21.8 Clauses that by their nature should continue after the Agreement ends, including clauses 7, 11, 16, 17, 19, 20, 21 and 24 and Schedule C, continue to apply.

22. CHANGES

22.1 Frabs may change these Terms from time to time. It will give the Customer at least 30 days' notice of any change, by email to the Account owner and in the Account, unless the change is needed sooner to comply with the law.

22.2 If a change is materially unfavourable to the Customer, the Customer may cancel under clause 21.2 before the change takes effect. If it does not, it accepts the change.

22.3 Frabs may change or withdraw features of the Service. If Frabs removes a feature that is a core part of the Product that the Customer has paid for, and does not replace it with something that does the same job, the Customer may cancel under clause 21.2.

22.4 A change to the Fees is dealt with under clause 6.7.

23. NOTICES AND COMMUNICATIONS

23.1 Frabs will send notices to the Customer by email to the Account owner and to the billing contact set in the Account, and may also show them in the Account. The Customer is responsible for keeping those contact details up to date.

23.2 The Customer may send notices to Frabs by raising a Ticket or by email to info@frabs.net. Reports of abuse coming from Frabs's own systems should also be sent to info@frabs.net.

23.3 A notice sent by email is treated as received at the time it is sent, unless the sender receives a message that it was not delivered.

23.4 Frabs sends system emails from addresses such as no-reply@frabs.net and alerts@frabs.net. These addresses are not monitored, and the Customer should use a Ticket to contact support.

23.5 Frabs will never ask for a password, an authenticator code, a recovery code or a sign-in code by email. The Customer should sign in only at frabs.net, at panel.frabs.net or at its own Custom Domain.

24. GENERAL

24.1 **Entire agreement.** The Agreement is the entire agreement between the parties about the Service and replaces all earlier discussions and documents about it. Each party confirms that it has not relied on any statement that is not in the Agreement. This does not limit liability for fraud.

24.2 **Assignment.** The Customer may not transfer or assign the Agreement without Frabs's written consent, which Frabs will not unreasonably withhold. Frabs may transfer the Agreement to a company that takes over its business, or to an Affiliate, by notice to the Customer.

24.3 **Subcontracting.** Frabs may use subcontractors, as set out in clause 3.5.

24.4 **Events outside a party's control.** A party is not in breach of the Agreement, and is not liable, for a delay or failure that is caused by an event outside its reasonable control, such as a failure of the public internet or of a power supply, natural disaster, war, terrorism, strike, cyber attack that could not have been prevented by reasonable security measures, or an order of a government. This does not excuse a failure to pay.

24.5 **Variation and waiver.** A change to the Agreement is valid only if it is in writing and agreed by both parties, or made under clause 22. A failure or delay in using a right is not a waiver of it.

24.6 **Severability.** If part of the Agreement is found to be invalid or unenforceable, the rest continues to apply, and the parties will replace the invalid part with a valid one that is as close as possible to its purpose.

24.7 **No partnership.** The parties are independent. Nothing in the Agreement makes them partners or agents of each other, and the partner programme in clause 6.5 does not create a legal partnership.

24.8 **Third parties.** Only the parties have rights under the Agreement. No one else, including an End Customer, may enforce it under the Contracts (Rights of Third Parties) Act 1999.

24.9 **Electronic acceptance.** The Agreement may be accepted electronically, including by clicking to accept when registering or in the Panel, and that has the same effect as a signature.

24.10 **Governing law and courts.** The Agreement, and any dispute or claim that arises from it or its subject, including a non-contractual dispute or claim, is governed by the law of England and Wales. The courts of England and Wales have exclusive jurisdiction over any such dispute or claim.

SCHEDULE A

FEES

A.1 The Fees below apply from the date of these Terms. The subscription is monthly and renews automatically until it is cancelled. Fees are per License per month, in US dollars, and do not include VAT. Payments are made through Stripe, and Fees are not refundable, as set out in clause 7.

Product	Tier	Licenses of that Product	Fee per License per month	Monthly minimum
Frabs Server	Tier 1	1	$9	$9
Frabs Server	Tier 2	2 to 5	$8	$9
Frabs Server	Tier 3	6 to 19	$7	$40
Frabs Server	Tier 4	20 or more	$6	$133
Frabs Host	Tier 1	1	$13	$13
Frabs Host	Tier 2	2 to 5	$12	$13
Frabs Host	Tier 3	6 to 19	$10	$60
Frabs Host	Tier 4	20 or more	$9	$190
Frabs Hypervisor	Tier 1	1	$17	$17
Frabs Hypervisor	Tier 2	2 to 5	$15	$17
Frabs Hypervisor	Tier 3	6 to 19	$13	$75
Frabs Hypervisor	Tier 4	20 or more	$11	$247

A.2 A License covers one Protected Server, as defined in clause 1.1. A Frabs Hypervisor License covers the virtualisation host and every supported virtual server on it, and is not charged per virtual server. For each Product, the monthly Fee is the number of Licenses of that Product multiplied by the rate for its Tier, or the Tier's monthly minimum if that is higher, so that a larger number of Licenses never costs less than a smaller one. For example, 8 Frabs Server Licenses are charged at $7 each, $56 a month.

A.3 Every Tier includes every feature of its Product, including network protection and resource abuse protection.

A.4 The free Trial is for one License of one Product, once for each company, as set out in clause 5. It continues into a paid subscription at that Product's Tier 1 Fee unless the Customer cancels before the Trial Period ends.

A.5 Partners approved under the partner programme receive the discount in clause 6.5 on their Frabs Host and Frabs Hypervisor Licenses.

A.6 A Customer that subscribed before the date of these Terms keeps the Fees and allowances it already has until Frabs gives notice of a change under clause 6.7.

SCHEDULE B

SUPPORT

B.1 Support is given through Tickets, as set out in clause 13. Support Hours are 09:00 to 18:00 UK time, Monday to Friday, excluding public holidays in England.

B.2 The targets below are for the first reply to a Ticket, counted in Business Hours within Support Hours, and depend on the total number of Licenses the Customer holds across all Products. They are targets and are not guaranteed.

Licenses held	First reply target
1	48 Business Hours
2 to 5	24 Business Hours
6 to 19	8 Business Hours
20 or more	4 Business Hours

B.3 Ticket priorities are Low, Normal, High and Urgent. Frabs sets the priority. A High or Urgent Ticket is looked at before a Normal or Low one, and the same first reply targets apply.

B.4 The Ticket statuses are Open, Waiting on Frabs, Waiting on customer, Solved and Closed. A Ticket that is Solved closes automatically after 7 days, as set out in clause 13.6.

SCHEDULE C

DATA PROCESSING

C.1 This Schedule applies whenever Frabs processes Customer Personal Data on the Customer's behalf in providing the Service. It replaces the separate Frabs Data Processing Agreement. Words such as controller, processor, data subject, personal data breach and processing have the meanings given in Data Protection Law.

C.2 **Roles.** The Customer is the controller of the Customer Personal Data and Frabs is its processor. If the Customer is itself a processor for its End Customers, it confirms that it is authorised to give Frabs the instructions in this Schedule and to appoint Frabs as its sub-processor.

C.3 **Instructions.** Frabs will process Customer Personal Data only on the Customer's documented instructions, which are these Terms, the Customer's use of the Service and its settings, and the Documentation. Frabs may also process it where the law requires, and will tell the Customer before it does so unless the law prevents it. Frabs will tell the Customer if, in its opinion, an instruction infringes Data Protection Law.

C.4 **Customer responsibilities.** The Customer is responsible for having a lawful basis to give Frabs the Customer Personal Data; for giving its End Customers and others any notice that the law requires, including that their traffic and their Workloads' resource use are monitored and that resource use may be limited; for the accuracy of the information it gives to Frabs; for not sending Frabs the content of communications or special category data; and for its decisions on Approvals, automation rules and Remediation Actions.

C.5 **Personnel.** Frabs will make sure that every person who processes Customer Personal Data on its behalf is bound by a duty of confidentiality and has access only where it is necessary to provide the Service.

C.6 **Security.** Frabs will protect Customer Personal Data with the measures in Schedule E, and may update them as long as the overall level of protection is not reduced.

C.7 **Sub-processors.** The Customer gives Frabs general authorisation to use the Sub-processors listed in Schedule D. Frabs will give at least 30 days' notice before it adds or replaces a Sub-processor, by email to the Account owner and on frabs.net. The Customer may object on reasonable data protection grounds within those 30 days; Frabs will work with the Customer to find a solution, and if the objection cannot be resolved the Customer may cancel under clause 21.2. Frabs binds each Sub-processor to terms that give similar protection and remains responsible for its work.

C.8 **Data subject requests.** If a data subject asks Frabs to use a right in relation to Customer Personal Data, Frabs will pass the request to the Customer without undue delay and will not respond to it except to say that it has been passed on, unless the law requires otherwise. Frabs will give the Customer reasonable help, through the Panel and on request, to answer such requests.

C.9 **Personal data breaches.** Frabs will tell the Customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach that affects Customer Personal Data. The notice will say, as far as Frabs knows, what happened, the categories and approximate numbers of data subjects and records affected, the likely consequences, and the steps taken or proposed. Frabs will take reasonable steps to contain the breach and help the Customer to meet its duties to tell the Information Commissioner's Office and data subjects.

C.10 **Assistance.** Frabs will give the Customer reasonable help with data protection impact assessments and prior consultation of the Information Commissioner's Office, where they relate to the Service.

C.11 **International transfers.** Frabs processes Customer Personal Data in the United Kingdom and the European Economic Area, on servers in Amsterdam, the Netherlands. Frabs will not transfer it to a country without adequacy regulations unless an appropriate safeguard is in place, such as the UK International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses, and the Customer has been told under clause C.7.

C.12 **Audit.** Frabs will give the Customer the information it reasonably needs to show that Frabs has met this Schedule. If that is not enough, or a regulator requires it, the Customer may audit Frabs's processing on at least 30 days' written notice, during business hours, without disrupting the Service more than necessary, no more than once in any 12 months unless there has been a personal data breach, keeping what it learns confidential and at its own cost.

C.13 **Return and deletion.** Customer Personal Data is exported and deleted as set out in clause 21.6 and clause 21.7.

C.14 **Liability.** Frabs's liability under this Schedule is subject to clause 20 and counts towards the limit in clause 20.4. Nothing in this Schedule limits a liability that cannot be limited by law, or the rights of data subjects.

C.15 Details of the processing:

Item	Details
Subject matter	Providing the Service to the Customer
Duration	The Subscription Term and the Trial Period, plus the periods in clause 21.6 and clause 21.7
Nature of the processing	Collecting, storing, analysing, attributing, displaying and deleting Detection Data and related Customer Data
Purpose	To detect, attribute, investigate and help to remediate attacks on and abuse from the Customer's Protected Servers and network, and resource abuse on them, and to keep a record of it
Types of Personal Data	Network addresses (such as IP addresses of Protected Servers, Workloads and the systems they communicate with), ports, protocols, timings and traffic volumes, the CPU, disk and memory use of Workloads, identifiers for Workloads and End Customers that the Customer or its integrations provide, such as virtual server names, hosting account names and domain names, and the contact details of Authorised Users
Categories of data subjects	End Customers and their users, people who communicate with the Customer's Protected Servers and Workloads, and the Customer's Authorised Users
Special category data	Not intended. The Customer must not send it to the Service
Content of communications	Not collected. The Sensor analyses flow metadata, abuse indicators and resource use readings, not the content of traffic, files or memory

SCHEDULE D

SUB-PROCESSORS AND SERVICE PROVIDERS

D.1 Sub-processors of Customer Data. The Customer agrees that Frabs may use the following Sub-processors:

Sub-processor	What it does for Frabs	Location
Leaseweb Netherlands B.V.	Hosts the servers that run the Panel, the API, the database and the mail system. Customer Data is stored and processed there	Amsterdam, the Netherlands
Cloudflare, Inc.	Only for Accounts that use a Custom Domain: routes the Panel at the Custom Domain and provides its TLS certificate. Panel traffic at the Custom Domain passes through its network	Global network

D.2 Other service providers. These companies are used for other parts of the business. They do not receive Customer Data:

Company	What it does for Frabs	Data involved	Location
Stripe (Stripe Payments Europe, Limited and its affiliates)	Takes payment for subscriptions and issues payment receipts	Billing name, billing address, billing country and payment details that the Customer gives to Stripe	Ireland, and other locations as Stripe states
Resend	Sends Frabs service emails, such as sign-in codes, invoices and Ticket notifications	Recipient email addresses and the email sent	United States and the European Union
Cloudflare, Inc.	Protects the registration and contact forms and the sales chat from bots	IP address and browser details of visitors	Global network
Google	Google Analytics on frabs.net, only for visitors who accept it	Website visit data, as described in the Frabs Privacy and Cookie Notice	Global

D.3 Frabs will update this Schedule in line with clause C.7.

SCHEDULE E

SECURITY MEASURES

E.1 Frabs applies the following measures. They describe what is in place at the date of these Terms.

Area	Measures
How the Service is built	The Sensor runs on the Protected Server and, on a virtualisation host, at the hypervisor level. Nothing is installed inside an End Customer's virtual server. The Sensor reads flow metadata, abuse indicators and resource use, not the content of traffic, files or memory. Protected Servers connect out to Frabs over HTTPS, and nothing connects in. Updates and policies are signed by Frabs and checked by the Sensor
Separate systems	The website and Panel, the API, the database, the mail system and a management server are separate servers. The database and the operations console are not reachable from the public internet
Access to the Panel	Multi-factor authentication for every Authorised User, with recovery codes. Roles of owner, admin, analyst and read-only limit what each person can do. An email is sent when a new device signs in
Access by Frabs	Operators sign in with passkeys on a separate sign-in system. Administrative access is only through one management server over an encrypted private tunnel. Views of a Customer's Account are read-only, need a recorded reason, are limited in time and are shown in the Customer's audit log
Separation	Each Customer's data is separated from other customers' data, enforced in the database itself

Area	Measures
Encryption	Data is encrypted in transit with TLS, including at a Custom Domain, and between Frabs servers over encrypted private tunnels. Secrets such as integration keys are stored encrypted and are not shown in full after they are created
Logging and monitoring	A tamper-evident audit log records staff actions. Servers are monitored and logs are collected centrally
Backups	Backups of the database are taken regularly and kept separately from the live system
Email	Frabs emails are authenticated with SPF, DKIM and DMARC, contain no tracking, and never ask for a password or a code
Incidents	Security incidents are investigated, contained and recorded, and personal data breaches are reported as set out in clause C.9
Remediation	Remediation Actions are taken only on an Approval or an automation rule, recorded in the audit log, and can be reversed in the Panel

E.2 Shared responsibility. The Customer keeps the Sensor up to date, secures its Protected Servers and its own systems, gives each Authorised User the lowest role they need, protects the devices and authenticator apps used to sign in, and reviews Approval requests carefully.

E.3 Reporting a vulnerability. Anyone who finds a security problem in Frabs can email info@frabs.net with "Security" in the subject line. Frabs will acknowledge the report and fix real problems as quickly as it can, and will not take legal action against anyone who reports in good faith, does not access or change data that is not their own, and gives Frabs a reasonable time to fix the problem before telling others.

End of Frabs Terms and Conditions · FRABS_TC_V.5 OCTOBER 2026