

Terms and Conditions (Supplier Terms)

Safety Software as a Service (SaaS)

Structure of these Supplier Terms

These Supplier Terms contain provisions that are specific to the provision of SaaS. At the end of the General Provisions there are product-specific Annexes, which set out additional product/service specific provisions (which also override the General Provisions if there is any conflict). There are Annexes for:

- ResponseEye
- DocDefender
- NEC Detention Officer Insights
- NEC Fire Survival Guidance ("FSG") Insights

At the end of the Supplier Terms is a Glossary; any capitalised terms within these Supplier Terms which are not defined in the Glossary shall have the meaning set out elsewhere in this Agreement.

General Provisions

Introduction

"**SaaS**" means software as a service. Each Buyer who subscribes for SaaS is given a right of access to the Supplier's applicable proprietary application software ("**Software**"), via a supported web browser, for the duration of the SaaS Term. Buyers are not granted a licence to the Software.

The Software is hosted by NTT United Kingdom Limited ("NTT") on Supplier's behalf on a third party's public cloud. The Buyer consents to the use of NTT as a sub-processor of personal data for the purpose of providing cloud services.

NEC's SaaS solutions:

- run on the latest, tested and approved version of the Software;
- unless otherwise stated in the product-specific Annex, are multi-tenanted which means many buyers using the same executables and database;
- run on a single version of the Software which is used by all SaaS Buyers; and
- comprise the right to use the Software and the Documentation and the right to access Software support services, as described below. The Buyer does not have to host the Software or install it on its own premises/hardware.

Onboarding Services for SaaS

The Supplier (as defined in the Particulars) shall deliver the Onboarding Services specified in the Particulars.

Unless expressly stated otherwise in the Particulars, the parties recognise that any Onboarding Services and Professional Service days set out in this Agreement are an estimate based on the parties' current understanding of their requirements and obligations.

Subject to the paragraph below, the Supplier will use reasonable endeavours to accommodate rescheduling of Onboarding Services and Professional Services at the Buyer's request. However, if the Buyer seeks to reschedule or postpone Professional Services or Onboarding Services within: (a) ten to six Business Days of the booked date for delivery, the Supplier shall be entitled to invoice the Buyer for 50% of the relevant charges; or (b) five Business Days or less of the booked date for

delivery, the Supplier shall be entitled to invoice the Buyer for 100% of the relevant Charges. All days paid for must be utilised within 12 months of the date of the Buyer's Purchase Order.

If the Buyer seeks to postpone Onboarding Services or Professional Service days at any time where the Supplier has booked a flight or incurred other reasonable expenses which are non-refundable, the Buyer will still be liable to pay the cost of such flight or other expenses.

Unless expressly stated otherwise in the Particulars, all SaaS shall be tested in accordance with the Supplier's standard test policies. Any additional testing activities that the Buyer requires the Supplier to carry out must be agreed in writing between the parties and may be chargeable. The Buyer shall be deemed to accept the SaaS, and such acceptance shall be irrevocable, if the SaaS is used by the Buyer in a live environment and/or for any live operations.

The Buyer shall be deemed to accept the deliverables set out in any Acceptance Certificate issued by the Supplier and such acceptance shall be irrevocable if the Buyer does not provide any written notification to the contrary and has failed to sign the Acceptance Certificate within the time period set out within such Acceptance Certificate.

Access to and use of the SaaS

Subject to the Buyer complying with the restrictions set out in these Supplier Terms and the other terms and conditions in this Agreement, the Supplier shall grant to the Buyer a non-exclusive, non-transferable right to permit the Authorised Users to use the SaaS and the Documentation during the SaaS Term solely for the Buyer's internal business purposes.

The Supplier shall set up the Buyer within the SaaS application ("**SaaS Portal**") and grant the Buyer's Administrator access to the SaaS in the technologically appropriate manner either by provision of a licence key, by granting access to a downloadable app, or by means of issuing a user name and password for the SaaS portal which can be accessed through such URL as may be notified by the Supplier from time to time.

The Buyer's Administrator shall then be permitted to access the SaaS through the SaaS Portal and it shall be the Buyer's Administrator's responsibility to configure the set-up of the SaaS, within the parameters set out within the Documentation, to reflect the Buyer's own policies and practices on application assessment and decision making.

The Buyer's Administrator, in accordance with the Documentation, shall be permitted to set up further users authorised to access the SaaS on behalf of the Buyer up to the numerical limit stipulated in the Particulars (if applicable). It is the Buyer's Administrator's responsibility to set the controls on and levels of access for each further user authorised. For the avoidance of doubt, the Buyer's Administrator and the further users set up by the Buyer's Administrator under this paragraph shall be the "Authorised Users" for the purposes of this Agreement.

In relation to the Authorised Users, the Buyer undertakes that:

- each Authorised User shall keep a secure password for their use of the SaaS and Documentation, that such password shall be kept confidential and shall be changed no less frequently than every 90 days; and
- it shall permit the Supplier to audit the SaaS. Such audit may be conducted no more than once annually, at the Supplier's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Buyer's normal conduct of business. If any of the audits referred to in this paragraph establishes that any unauthorised access has occurred or that passwords have been provided to individuals who are not Authorised Users, then without prejudice to the Supplier's other rights, the Supplier reserves the right to (i) charge the Buyer for the costs of performing the audit(s), and/or (ii) recover the charges which would have been due to the Supplier had the Supplier licensed such additional Use; and/or (iii) disable such passwords and shall not issue any

new passwords to such individuals (unless or until the appropriate charges due in respect of any additional concurrent or named users have been paid).

In relation to the Buyer's Administrator, the Buyer undertakes that:

- the Buyer's Administrator will review and act upon any update information or reasonable instructions of the Supplier, including disseminating such applicable update information and instructions to other Authorised Users; and
- the Buyer's Administrator shall monitor the Authorised Users and ensure that they act in accordance with the terms of this Agreement.

The Buyer and its Authorised Users shall not access, store, distribute or transmit any Viruses, or any material during the course of its use of the SaaS that:

- is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- facilitates illegal activity;
- depicts sexually explicit images;
- promotes unlawful violence;
- is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or
- is otherwise illegal or causes damage or injury to any person or property;

and the Supplier reserves the right, without liability to the Buyer, and without prejudice to any other rights of the Supplier (whether under the Agreement or otherwise), to disable the Buyer's access to any material that breaches the provisions of this paragraph.

The paragraph above shall not apply to the extent only that the SaaS is specifically designed for such purposes and is being used lawfully including for the prevention and/or detection of criminal activity.

The Buyer and its Authorised Users shall not:

- attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the SaaS, except:
 - ➔ as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties; and
 - ➔ to the extent expressly permitted under this Agreement;
- attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the SaaS and/or Documentation (as applicable) in any form or media or by any means; or
- access all or any part of the Services and Documentation in order to build a product or service which competes with the SaaS and/or the Documentation; or
- use the SaaS and/or Documentation to provide services to third parties (the Buyer's citizens shall not be deemed to be third parties for the purposes of this paragraph); or
- license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the SaaS and/or Documentation available to any third party except the Authorised Users, or
- attempt to obtain, or assist third parties in obtaining, access to the SaaS and/or Documentation, other than as provided under this paragraph.

The Buyer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the SaaS and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify the Supplier.

The Buyer shall access the SaaS via a supported web browser or as may be otherwise agreed between the parties.

Media recorded during the SaaS Term will remain on the SaaS Portal for 30 days after its recording date and personal identifiable information (e.g. caller's phone number and GPS coordinates) will remain on the SaaS Portal for 90 days after the recording date.

The Supplier will use reasonable commercial endeavours to accommodate the introduction of substantive legislative changes. The Supplier expressly reserves the right to charge for the provision of any such substantive legislative updates where: (a) the development of the update is in the reasonable opinion of the Supplier technically complex; and (b) the costs of developing the update are in the reasonable opinion of the Supplier sufficient to warrant a charge for the provision of the update to the Supplier's buyers at large.

Security, Disaster Recovery and Back-up Policy

The Buyer shall own all right, title and interest in and to all of the Buyer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Buyer Data.

Unless otherwise expressly stated in an Annex in relation to a particular SaaS product, the Supplier confirms that:

- the SaaS platform is designed and implemented in accordance with the 27001 baseline control set, the National Cyber Security Centre (NCSC) Top Ten and the NCSC Cloud Security Principles. The environment from which the SaaS shall be delivered conforms to the relevant sections of the Government Security Policy Framework and Personnel Security Controls and to all relevant Communications Electronics Security Group Memoranda, Manuals and Standards;
- it shall comply with the Supplier's Privacy and Security Policy relating to the privacy and security of the Buyer Data;
- its information security management system is certified to ISO 27001 and ISO 27002;
- its quality management system is certified to ISO 9001:2015;
- its service management system operates in accordance with the ITIL framework;
- it conducts application penetration testing by internal testers, the results of which will be shared with the Buyer upon request; and
- the information assurance process as detailed within the paragraphs above will be periodically revised and updated to ensure alignment with good industry practice.

The Buyer recognises that the SaaS is a hosted, multi-tenanted solution unless stated otherwise in the product-specific Annex. The Buyer Data will be segregated from the data of other buyers using the SaaS and there will be no data sharing facility.

The Supplier confirms that it uses more than one data centre with separate infrastructure and resilience for provision of the SaaS to ensure relocation of the SaaS provision in the event of non-availability of one data centre.

The Supplier confirms that its disaster recovery and business continuity policies, processes and procedures are based on standard BS25999 and ISO 22301:2019.

The Back-Up Policy is as follows:

- the Supplier takes multiple back-ups within the system as part of the SaaS;
- in the event of any loss or damage to Buyer Data, the Buyer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial endeavours to restore the lost or damaged Buyer Data from the latest back-up of such Buyer Data maintained by the Supplier; and
- the Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Buyer Data caused by any third party (except those third parties sub-contracted by the Supplier to perform services related to Buyer Data maintenance and back-up).

Buyer Obligations

Except where the Supplier has specifically agreed to provide such services the Buyer will:

- be responsible for the operation and use of the SaaS and any associated documentation and the results obtained from these;
- supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement; and
- provide the Supplier's personnel with full free and safe access to its site where required, to enable the Supplier to perform its obligations under this Agreement.

The Buyer shall in good faith:

- provide the Supplier with (i) all necessary co-operation in relation to this Agreement; and (ii) all necessary access to such information as may be required by the Supplier in order to provide the SaaS, including but not limited to Buyer Data and security access information;
- comply with all applicable laws and regulations with respect to its activities under this Agreement;
- carry out all other Buyer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the Buyer's provision of such assistance as agreed by the parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary and reserves the right to charge the Buyer for any costs incurred by the Supplier as a consequence of such delay;
- ensure that (where applicable) the Authorised Users use the SaaS and the Documentation in accordance with the terms and conditions of this Agreement and shall be responsible for any Authorised User's breach of this Agreement;
- obtain and shall maintain all necessary licences, consents, and permissions necessary for the Supplier, its contractors and agents to perform their obligations under this Agreement, including without limitation the SaaS;
- ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time; and
- unless expressly stated otherwise in the Particulars, be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Supplier's public or private cloud (as applicable), and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Buyer's network connections or telecommunications links or caused by the internet.

SaaS Support Services

The Buyer's Support Team shall provide the following services:

- Infrastructure support up to the SaaS boundary
- Receive Calls from Authorised Users
- Apply the Buyer's service management processes
- Request Fulfilment (i.e. respond to Service Requests) comprising:
 - System administration
 - Application configuration including CV lists, creation of users
 - Deal with "how do I?" enquiries
 - Configure additional users
- Incident Management comprising:
 - Address data quality issues
 - Observe and accurately record symptoms of an Incident including any testing and subsequent results
 - Triage Incidents to establish that the SaaS is the likely cause of an Incident
 - Carry out work on-site to assist the Supplier Support Team in further diagnostics
 - Simple investigation and Resolution using diagnostic tools / log files
 - Facilitate Resolution by switching to a standby system (if applicable) or from backups or implement a temporary work-around and continue work to apply a permanent Resolution
 - Notify the Supplier of any Incident which has been resolved and the steps taken to resolve
- Knowledge Management comprising:
 - Application of available knowledge
 - Generation and maintenance of knowledge articles

Should the Buyer's Support Team be unable to resolve an Incident or fulfil a Service Request, a Call shall be logged with the Supplier. During the SaaS Term the Supplier shall, as part of the SaaS and at no additional cost to the Buyer, provide the Buyer's Support Team access to the Supplier's Service Desk which operates 24x7x365 for recording details of Calls. The Buyer's Support Team can use the following methods to contact the Service Desk:

- Telephone (Priority Levels P1, P2, P3, P4 and Service Request);

When contacting the Service Desk to report a Call, the Buyer's Support Team shall provide the following information:

- Caller name (and further contact details if required);
- Name and contact details of the Authorised User experiencing the issue (if applicable);
- Priority;
- A description of the issue including the steps to replicate; and
- A description of the urgency and impact of the issue.

Once these details have been entered into the Supplier's IT service management tool, the Supplier will provide the Buyer's Support Team with a Call reference number, which shall be quoted by the Buyer's Support Team in all further communication with the Supplier in connection with the Call.

Once Calls have been logged, they are passed to a software support team for Resolution (the **"Supplier Support Team"**) during Normal Support Hours for Priority Levels P3 and P4, and 24/7/365 for Priority Levels P1 and P2.

At any stage during the lifecycle of a Call the Buyer's Support Team can enquire on progress status by contacting the Service Desk and quoting the relevant Call reference number.

The Supplier Support Team shall provide:

- Remote support services as detailed in these Supplier Terms;
- New Releases, which may be subject to additional charges;
- Software Patches to resolve incidents/problems; and
- Service Packs as they are made generally available which may be subject to an additional charge if they include new functionality.

The provision of the Support Services is subject to the Buyer providing such information as is reasonably necessary to enable the Supplier to diagnose any Incidents or Problem in the SaaS.

Service Levels

Calls logged with the Service Desk will be allocated to the Supplier Support Team for Resolution during Normal Support Hours. The Particulars shall specify whether 24x7 support for P1 and P2 Incidents shall apply.

Incidents and Service Requests are processed on a Priority Level basis. The Supplier will verify the Priority Level assigned by the Buyer's Support Team on the Call, by reference to the applicable Annex, and the parties will agree a revised Priority Level if appropriate. The final decision on the Priority Level will remain with the Supplier.

In order to perform Incident investigation and Service Request fulfilment, the Supplier may require access to the Authorised User experiencing the issue. The Buyer shall promptly provide such access as and when reasonably requested.

As Calls are progressed, the Supplier will record details of all its contact with the Buyer's Support Team and/or Authorised User.

Once a Call has been resolved, the Supplier Support Team or Service Desk will contact the Buyer's Support Team and the Call will only be closed if both parties are in agreement. Closed Calls cannot be reopened except with the consent of both parties. Should the Supplier not receive confirmation of closure after seven calendar days of requesting the same from the Buyer's Support Team, then the Supplier will automatically close the Incident.

When a Problem is identified which requires a change to the SaaS solution, a Problem will be recorded and a reference number supplied to the Buyer's Support Team; this needs to be quoted in all correspondence with the Supplier relating to that Problem. The corresponding Incident is then closed if a workaround is provided.

Measurement of the Response time begins at the earliest point in time during Normal Support Hours at which the Call is reported to the Service Desk, and will continue during Normal Support Hours. If a Call is reported outside of Normal Support Hours, the Response time will start to be measured at the beginning of the next Normal Support Hours period. Measurement of the Response time ends when the Supplier has contacted or attempted to contact, via any means, the Buyer's Support Team to acknowledge receipt of or further discuss a reported Call.

Measurement of the Resolution time begins at the earliest point in time during Normal Support Hours at which the Call is reported to the Service Desk, and will continue during Normal Support Hours. If a Call is reported outside of Normal Support Hours, the Resolution time will start to be

measured at the beginning of the next Normal Support Hours period. Measurement of the Resolution time ends when the Incident has been resolved and the workaround or permanent fix provided to the Buyer, or the Service Request has been fulfilled (as applicable).

The Supplier SLA clock is paused in certain circumstances including:

- while the Call is outside the scope or control of the Supplier; and
- outside Normal Support Hours; and
- while the Supplier is awaiting information from the Buyer's Support Team or Authorised User.

In addition, should Supplier personnel be required to attend site, this will be charged for on a time and materials basis in accordance with the rate card set out in the contract plus expenses.

The Supplier will not be liable for any service failure:

- for which the Supplier is not responsible; or
- which relates to an Additional Service; or
- which arises as a result of Incidents arising due to factors beyond the Supplier's reasonable control.

The Supplier shall use commercially reasonable endeavours to make the SaaS available to be accessed and used by the Buyer 99.9% of the time, measured during Normal Support Hours, excluding the following periods:

- planned maintenance (which shall be carried out at such times as are notified to the Buyer, by giving a reasonable period of advance notice); and
- unscheduled emergency maintenance carried out where there is an identified and demonstrable immediate risk to the SaaS solution.

Service credits shall not apply in the event of breach of the Service Levels.

Service reporting is not provided as part of SaaS.

Additional Services

Additional Services may be provided at the Supplier's sole discretion and may be subject to additional charges accruing on a time and materials basis based on the Supplier's then prevailing day rates, unless otherwise agreed.

The Support Services shall not include the diagnosis or rectification of any Incident which is not attributable to a Problem in the SaaS or which results from any of the following, the diagnosis or rectification of which shall all be considered Additional Services:

- improper use, operation or neglect of either the SaaS or the equipment and environment on which the Software is licensed for use; or
- modification of the SaaS or its merger (in whole or in part) with any other software, without the Supplier's prior written consent; or
- use of the SaaS on equipment other than the equipment supplied by the Supplier for use with the SaaS or on equipment which does not meet the minimum specification for hardware, operating system and/or Third Party Software published by the Supplier in accordance with the SaaS release information document; or
- failure by the Buyer to implement recommendations in respect of or solutions to Incidents or Problems previously advised by the Supplier; or
- any repair, adjustment, alteration or modification of the SaaS by any person other than the Supplier without the Supplier's prior written consent; or

- use of the SaaS for a technical purpose for which it was not designed; or
- a consequence of infrastructure components or network factors which the Supplier is not responsible for supporting; or
- a failure caused by any other factors outside the reasonable control of the Supplier; or
- any situation where a reasonably skilled and competent Authorised User would consider assistance from the Supplier to be unnecessary; or
- a consequence of any programming error, virus or disabling code set out in the Third Party Software; or
- use of SaaS on anything other than Edge or Chrome browsers, unless otherwise stated in the release documentation.

Variations

If a third party supplier to the Supplier increases the fees charged, the Supplier reserves the right at any time to pass these increases onto the Buyer.

The Supplier may, upon six months' prior written notice to the Buyer, modify the SaaS or any part thereof provided that there is no material degradation of the service.

Termination and Consequences of Termination

In the event the Supplier elects to withdraw a particular type of SaaS, it may do so without liability provided it has given the Buyer not less than six months' prior written notice. The Supplier shall, following the expiry of the SaaS Term, disable the Buyer's access to the SaaS.

On termination or expiry of the Agreement, the Buyer will not be able to log in to the SaaS Portal. Media recorded prior to the date of termination or expiry of the Agreement will remain on the SaaS Portal for 30 days after its recording date and personal identifiable information (e.g. caller's phone number and GPS coordinates) will remain on the SaaS Portal for 90 days after the recording date. During these periods the media or other session details may be retrieved by the Supplier following a request from the Buyer but the Buyer will not be able to access the records directly. The Buyer's account with configuration information and user accounts will be deleted manually by the Supplier on or after the date 90 days after the date of termination or expiry.

Additional Terms

Regardless of any other provision in the Agreement:

Specification

- if this Agreement contains the Buyer's service description, requirements and/or specification ("**Specification**") and if any provision of that Specification conflicts with these Supplier Terms, then these Supplier Terms will take precedence.

Buyer Policies and consents

- the Supplier's individual staff involved in providing the Services shall not be required to sign any Buyer provided IT remote access, usage or email policy documents.
- the Supplier shall not be required to enter into any separate or additional agreements or arrangements with the Buyer (or any third party that is not a subcontractor or sub-processor of the Supplier) in order to provide the Deliverables, including codes of connection, network/system access or data processing/sharing agreements.

Exclusions

- except to the extent not permitted by law, the Supplier shall have no liability under or in connection with this Agreement (whether in contract, tort (including negligence), under an indemnity, statute or otherwise), to the extent that any losses, damage or defects arise as a result of (but not limited to):
 - the late arrival or non-arrival of Buyer Data or other material from the Buyer;
 - errors or omissions in any information, data, instructions or scripts (including where the same is in the correct format) provided to the Supplier by the Buyer in connection with this Agreement;
 - any actions taken by the Supplier at the Buyer's direction;
 - failure to detect errors in any work performed by the Supplier which the Buyer has undertaken to check;
 - the act and/or omission of a third party (including a subcontractor and/or sub-processor but excluding any Group Company) unless and to the extent only that the third party is liable to the Supplier for such act/omission; or
 - any other act or omission of the Buyer (or third parties appointed by or under its control) including but not limited to failure of communication links.
- the Buyer assumes sole responsibility for results obtained from its use of the Deliverables and for any conclusions drawn from such use.

Transfer of employees

- the Buyer warrants, represents and undertakes to the Supplier that there will be no relevant transfer for the purposes of the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ("**TUPE**") of employees from the Buyer (or any supplier, contractor or other service provider to the Buyer) to the Supplier (or any third party supplier/subcontractor to the Supplier). Regardless of any other provision of this Agreement, the Buyer agrees to indemnify the Supplier against all costs, claims, liabilities and expenses (including reasonable legal expenses) incurred by the Supplier in connection with or as a result of:
 - a claim by any person who transfers or alleges that they have transferred to the Supplier (or any third party supplier/subcontractor to the Supplier) as a result of entering into this Agreement; and/or
 - any failure by the Buyer to comply with its obligations under regulations 13 and 14 of TUPE, or any award of compensation under regulation 15 of TUPE.

Intellectual Property Rights

- the provisions in this Intellectual Property section shall not apply to any software provided by the Supplier.
- the Buyer acknowledges that the Supplier and/or their respective licensors own Intellectual Property Rights in any specifications, data, databases, documentation, and other materials provided to the Buyer as part of the Services. Except as expressly stated in these Supplier Terms, the Supplier does not grant the Buyer any rights to, or in, the Intellectual Property Rights in respect of the above materials.
- the Supplier grants the Buyer a non-transferable, non-exclusive right during the term of this Agreement to use the materials supplied by the Supplier under the Services for its own internal business purposes. Where the Agreement expressly states that Buyer is procuring

the Deliverables on behalf of or for the benefit of a specified third party end customer, the licence granted in this paragraph applies to that end customer and allows them to use the materials for that end customer's own internal business purposes.

- all Intellectual Property Rights in the Buyer Data and any other materials provided to the Supplier by the Buyer for the Supplier to provide the Services will remain vested in the Buyer. The Buyer grants the Supplier a perpetual, royalty free, non-exclusive licence to use (and copy) the Buyer Data to perform this Agreement and to comply with any requests made to the Supplier under statute.

Certifications and Accreditations

- the Supplier's certifications and accreditations are as set out at [Certificates and Registrations - NEC Software Solutions](#), as updated by the Supplier from time to time.

Third Party Deliverables

- in the event that a third party suspends or terminates (or gives notice to suspend or terminate) the provision of any Deliverable(s) to the Supplier for any reason, then the Supplier shall be entitled to suspend or terminate the provision of such Deliverable(s) to the Buyer under this Agreement.

Offshore Resource

- in some circumstances we may use resources provided by one or more of our Group Companies, including those of our Group Company NEC Software Solutions India PVT Limited. This may involve sharing your data (including Personal Data) with them, processing, or transferring your data outside the UK. Whenever we use the resources of our Group Companies, and/or process or transfer your data out of the UK, the terms of our Agreement with you, including applicable legislation, as well as our internal policies, procedures and processes shall apply. At all times we retain responsibility for ensuring compliance by our Group Companies with our obligations. By entering into this Agreement you consent to the use of our Group Companies' resources (including NEC Software Solutions India PVT Limited) to provide the Deliverables, and/or to process your data (including Personal Data).

Sub-processors

- in addition to the specific authorisation above, the Buyer also grants to the Supplier general authorisation to engage Sub-processor(s) as third-party Processors of Personal Data under this Agreement. A list of the Supplier's Sub-processors that the Supplier directly engages for the specific Deliverables as a Sub-processor from time to time is available at **[www.necsws.com\subprocessors](http://www.necsws.com/subprocessors)**. Any changes to the list of the Supplier's Sub-processors will be updated via this link.

Annex: NEC ResponseEye

Where NEC ResponseEye is to be provided the provisions set out in this Annex shall apply. If there is any conflict between the provisions set out in this Annex and the General Provisions above, this Annex shall apply.

Use of a third party's public cloud

The Buyer acknowledges that NEC ResponseEye is hosted in a third party environment provided by Microsoft Azure ("MS Azure") using a cloud solution which, regardless of any other provision in this Agreement, shall be provided in accordance with MS Azure's standard terms & conditions as at the date of signature of the Agreement to the exclusion of all other terms, including in relation to service availability and support. For clarity, the only Service Levels that shall apply to the hosting platform component of NEC ResponseEye are those provided by MS Azure.

The Buyer consents to the use of MS Azure as a sub-processor of personal data for the purpose of providing cloud services and acknowledges and agrees to the provision of those services on MS Azure standard terms.

Service Levels

All target times specified in the table below are measured within the Normal Support Hours. Maintenance Cover Time (MCT) is Mon - Fri 08:00 - 18:00hrs excluding UK Public Holidays

Service Levels for ResponseEye			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that the ResponseEye is unable to be used by all users.	15 mins	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	15 mins	8 hours
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	30 mins	48 hours

P4	Low. Comprising: Issue affecting a single Authorised User	30 mins	96 hours or next scheduled release
Service Request	For example: requests for information, advice and/or guidance.	1 working Day	None

Annex: NEC DocDefender

Where NEC DocDefender is to be provided the provisions set out in this Annex shall apply. If there is any conflict between the provisions set out in this Annex and the General Provisions above, this Annex shall apply.

Overview

- NEC DocDefender is a software application that is provided as a service over the internet to help users remove personal identifiable information (PII) and other sensitive information from digital documents. This tool is designed to provide an efficient and accurate method of redacting information from documents, without requiring significant manual effort or specialised skills.
- The tool uses algorithms to scan documents, identify and redact sensitive information, such as names, bank account details or personal addresses. Users are responsible for reviewing the output document and making any adjustments as needed to ensure the output is accurate.

The Supplier is committed to providing an industry-leading service that is valuable and easy to use for all users. DocDefender has been designed to be used without any training.

Use of a third party's public cloud

The Buyer acknowledges that NEC DocDefender is hosted in a third party environment provided by Amazon Web Services ("AWS") using a public cloud solution which, regardless of any other provision in this Agreement, shall be provided in accordance with AWS's standard terms & conditions as at the date of signature of the Agreement to the exclusion of all other terms, including in relation to service availability and support. For clarity, the only Service Levels that shall apply to the AWS hosting platform component of NEC DocDefender are those provided by AWS.

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services and acknowledges and agrees to the provision of those services on AWS' standard terms.

Without prejudice to the above, the "Offshore Resource" section set out in the General Provisions section of this document, does not apply.

Access and Use of DocDefender

DocDefender is licensed for use by the Buyer organisation, there is no limit on the number of Authorised Users. Authorised Users are authenticated using their Microsoft authentication solution – for clarity the Supplier does not issue or manage any specific user accounts, details or passwords.

The following provisions set out in the General Provisions section of this document do not apply:

*"The Buyer's Administrator, in accordance with the Documentation, shall be permitted to set up further users authorised to access the SaaS on behalf of the Buyer up to the numerical limit stipulated in the Particulars (if applicable). It is the Buyer's Administrator's responsibility to set the controls on and levels of access for each further user authorised. For the avoidance of doubt, the Buyer's Administrator and the further users set up by the Buyer's Administrator under this paragraph shall be the **"Authorised Users"** for the purposes of this Agreement.*

If there is an End User named in the Particulars, the Supplier grants the Buyer the right to access and use the SaaS for the benefit of such End User.

In relation to the Authorised Users, the Buyer undertakes that:

each Authorised User shall keep a secure password for his/her use of the SaaS and Documentation, that such password shall be kept confidential and shall be changed no less frequently than every 90 days; and

it shall maintain a written, up to date list of the current Authorised Users and provide such list to the Supplier within five Working Days of the Supplier's written request at any time or times."

Support Services and Service Levels

Support Service

DocDefender has in-built guidance, training videos and an automated chatbot for self-service support. Authorised Users also have access to an email address to reach out to the Supplier directly for support during Normal Business Hours. User accounts, authentication and access management are handled by customers using their identity provider, e.g. Azure Active Directory.

For clarity, the Service Desk facility described in the General Provisions section of this document above, is not part of the Support Service for DocDefender.

Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC DocDefender			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that the NEC DocDefender SaaS is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days

P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

Alerts and Monitoring

The Supplier continually monitors DocDefender to ensure it is operating as expected and receives alerts for abnormal activity.

Supplier Management

If requested, service reviews between the Supplier and key Buyer stakeholders to review high level metrics and feedback can be conducted monthly for an initial term (3 months) followed by quarterly. DocDefender includes the ability for the Buyer to view high-level management information regarding the use of the platform. This management information can be discussed during service reviews as well as new features implemented within the system and any major items in the roadmap for next period.

Fair Use Policy

The following Fair Use Policy applies to the use of DocDefender:

- **Fair Usage:** The usage limit is specified in the Particulars ("Usage Limit") and usually expressed as a maximum number of pages per annum that can be processed and redacted using DocDefender and is designed to ensure fair usage of the SaaS as well as preventing abuse or excessive consumption of system resources-
- **Usage Limit:** The Buyer is permitted to process and redact documents subject to remaining within the Usage Limit without incurring additional charges.
- **Extra Charges:** If the Usage Limit is exceeded, an additional fee of £0.05 per page ("Extra Charges") shall be payable for each additional page processed beyond the limit.
- **Calculation of Pages:** Pages are counted based on the number of pages processed through the SaaS, regardless of their size or content. Each individual page within a document is considered as one page. It is the responsibility of the Customer to monitor their page usage within the SaaS.
- **Notification of Extra Charges:** If the Buyer exceeds the Usage Limit, the Supplier will notify and invoice the Buyer of the overage and the associated Extra Charges.
- **Payment of Extra Charges:** Extra Charges for exceeding the Usage Limit will be invoiced separately. Failure to pay the Extra Charges shall entitle the Buyer to suspend or terminate the SaaS.

If the Buyer organisation increases in size by more than 10%, they shall inform the Supplier who will provide a revised quote based on the increased size of the Buyer. Continued access to and use of DocDefender is subject to payment of the revised Charges.

Buyer's obligations

In addition to any other obligations of the Buyer stated elsewhere in the Agreement:

- the Buyer is responsible for obtaining and will ensure that it holds all necessary licences, permissions and consents required in order for the Supplier to process the documents provided by the Buyer, using DocDefender, including the necessary licences for the fonts used within such documents and ensuring that documents marked 'Secret' or 'Top Secret' are not processed using DocDefender;
- the Buyer will ensure that Authorised Users understand that in relation to any redaction of documents, DocDefender provides suggestions only: Authorised Users remain the ultimate decision maker and shall be responsible at all times for checking the redaction output of documents; and

- the Buyer will keep secure all log in information for the use of the SaaS.

Annex: NEC Detention Officer Insights

Where NEC Detention Officer Insights is to be provided the provisions set out in this Annex shall apply. If there is any conflict between the provisions set out in this Annex and the General Provisions above, this Annex shall apply.

Use of a third party's public cloud

The Buyer acknowledges that NEC Detention Officer Insights is hosted in a third party environment provided by Amazon Web Services ("AWS") using a public cloud solution which, regardless of any other provision in this Agreement, shall be provided in accordance with AWS's standard terms & conditions as at the date of signature of the Agreement to the exclusion of all other terms, including in relation to service availability and support. For clarity, the only Service Levels that shall apply to the AWS hosting platform component of NEC Detention Officer Insights are those provided by AWS.

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services and acknowledges and agrees to the provision of those services on AWS' standard terms.

Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Detention Officer Insights			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that NEC Detention Officer Insights is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day

P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

Annex: NEC Fire Survival Guidance (FSG) Insights

Where NEC Fire Survival Guidance (FSG) Insights is to be provided the provisions set out in this Annex shall apply. If there is any conflict between the provisions set out in this Annex and the General Provisions above, this Annex shall apply.

Use of a third party's public cloud

The Buyer acknowledges that NEC Fire Survival Guidance (FSG) Insights is hosted in a third party environment provided by Amazon Web Services ("AWS") using a public cloud solution which, regardless of any other provision in this Agreement, shall be provided in accordance with AWS's standard terms & conditions as at the date of signature of the Agreement to the exclusion of all other terms, including in relation to service availability and support. For clarity, the only Service Levels that shall apply to the AWS hosting platform component of NEC Fire Survival Guidance (FSG) Insights are those provided by AWS.

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services and acknowledges and agrees to the provision of those services on AWS' standard terms.

Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Fire Survival Guidance (FSG) Insights			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that the NEC Fire Survival Guidance (FSG) Insights is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day

P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

Glossary

In addition to the terms defined elsewhere in this Agreement, the following terms (regardless of any other provision in this Agreement) shall have the meaning set out below:

"Acceptance Certificate"	means a document issued by the Supplier following completion of a deliverable;
"Additional Services"	means any support, maintenance and other services which are outside the scope of the Support Services and which Supplier has agreed to provide;
"Agreement"	means the legally binding contract between the Supplier and the Buyer of which these Supplier Terms forms part;
"Authorised User(s)"	means those employees, agents and independent contractors of the Buyer who are authorised by the Supplier to use the SaaS and the Documentation;
"Back-Up Policy"	means the specific arrangements for the back-up of Buyer Data as set out in these Supplier Terms, as may be amended from time to time by the Supplier in its sole discretion upon reasonable prior written notice;
"Business Day"	means any day which is not a Saturday, Sunday or bank or public holiday in England and Wales;
"Buyer's Administrator"	means the person duly appointed by the Buyer to act as its administrator and the Supplier's lead contact for the purposes of the SaaS, as notified by the Buyer to the Supplier;
"Buyer's Support Team"	means those employees, agents and independent contractors of the Buyer who are authorised by the Supplier to use the Supplier's support service;
"Buyer Data"	means the data inputted by the Buyer, or Authorised Users for the purpose of using the SaaS or facilitating the Buyer's use of the SaaS;
"Call"	means notification of an Incident or Service Request by an Authorised User to the Service Desk in accordance with these Supplier Terms;
"Group Company"	means the Supplier, each and any subsidiary or holding company from time to time of that company, and each and any subsidiary from time to time of a holding company of that company. A "holding company" and "subsidiary" shall have the meaning as set out in section 1159 of the Companies Act 2006;

"Incident"	means any event which is not part of the standard operation of the SaaS and which causes, or may cause an interruption to, or a reduction in, the quality of that software or service;
"Normal Support Hours"	means Monday to Friday 09:00 to 17:30 (eight and a half hours) UK time, each Business Day;
"Particulars"	means the document entitled "Particulars" to which these Supplier Terms is attached, and if there is no such document, that part of the Agreement setting out the key details of the Deliverables and the amounts payable therefor;
"Priority Level"	means the priority level of the Call reasonably specified by the Buyer's Support Team, and agreed by the Supplier, according to the criteria set out in the applicable Annex;
"Problem"	means the unknown underlying root cause of one or more Incidents;
"Privacy and Security Policy"	means the Supplier's policy relating to the privacy and security of the Buyer Data, as may be amended from time to time by the Supplier in its sole discretion, which is available on request;
"Resolution"	means action which will resolve an Incident which may be a Workaround. "Resolve" and "Resolved" shall be construed accordingly;
"Response"	means contact via any means made by the Supplier to the Buyer's Support Team or Authorised User in response to a Call reported via the Service Desk;
"SaaS"	means the Software as a Service to be provided by or on behalf of the Supplier to which the Buyer will be granted access and use in accordance with this Agreement;
"SaaS Portal"	has the meaning set out in these Supplier Terms;
"Service Desk"	means the Supplier's service desk detailed in these Supplier Terms;
"Service Level(s)"	means the service levels (as set out in these Supplier Terms) which apply in respect of the SaaS;
"Service Request"	means a Buyer's Support Team request for information or advice and guidance;
"Supplier Support Team"	means the Supplier's software support team which Resolves Calls;

"Support Services"	means the support and maintenance services which are provided by the Supplier as detailed in these Supplier Terms;
"Third Party Software"	means software which is proprietary to a party other than the Supplier (and which is not, for the avoidance of any doubt, the SaaS) and licensed to the Buyer by the Supplier;
"Virus"	means any thing or device (including any software, code, file or program) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices; and
"Workaround"	means a method of avoiding an Incident or Problem either by a temporary fix or by a technique that means the Authorised User is not reliant on a particular aspect of the SaaS that is known to have an issue.



© 2026-present day, NEC Software Solutions UK Limited or one of its group companies. These Supplier Terms are protected by copyright laws in England and other countries and must not be copied, stored in a retrieval system or transmitted in any form or by any means in whole or in part without the prior written permission of NEC Software Solutions UK Limited.