

G – Cloud 15

Service Definition

Version 1.0

IIS exists to provide world-class secure internet intelligence & investigation solutions to a carefully vetted collection of organisations.

Securely Deployed AI Capabilities

Contents

1.	Introduction	3
2.	Service Description	3
3.	Professional Services	5
4.	Onboarding and Offboarding Requirements	5
5.	Technical Requirements.....	6
6.	Security and Data Protection.....	7
7.	Support and Maintenance	7
8.	Customer Accounts and Usage Responsibilities.....	8
9.	Additional Information	9

1. Introduction

1.1 Overview of the G-Cloud Service

This document presents Internet Investigation Solution Ltd.'s ("IIS") securely deployed AI Capabilities.

For more information on the services we offer please consult our secure website at the following URL:
ii-solutions.co.uk

1.2 Company Overview

Internet Investigation Solutions Ltd ("IIS") is a proud subsidiary of The Investigo Group® Ltd ("TIG"). Within our group, Vestigo Consulting Ltd ("Vestigo"), Collaboraite Ltd ("Collaboraite") and Voix Telecom Ltd ("Voixtel®") also operate as key subsidiaries, each dedicated to excellence within their respective domains. Together, our group companies provide a comprehensive suite of complementary products and services designed to meet the diverse needs of our customers. Collaboraite leads on the development of the group's secure and operationally focused advanced analytics and AI tools.

2. Service Description

2.1 Collab.hq

Collab.hq is the home to the Collaboraite AI tools. Each AI model available through Collab.hq is developed in-house by security cleared software and AI specialists. Collab.hq is a completely containerised capability where the models do not utilise public cloud cognitive services. This means the data being analysed is neither being stored in third party environments, nor being used to train collab.hq or unknown party models.

Collab.hq delivers privately hosted, secure AI-powered triage tools for video, audio, image and text including transcription (Collab.tcb), translation (Collab.trl), and object detection (Collab.obj), helping organisations overcome capacity and capability challenges. Users can upload files from their investigations or intelligence gathering for analysis. Results can be exported for verification, saving significant time and cost. Additional models are continuously added such as OCR, text-to-text and entity matching, with features accessed via a single standardised credit system.

The models can be used together or independently. New features will be made available via Collab.hq automatically for users to access, using credits to access the features relevant to their role.

Collab.hq can be deployed in two different ways.

2.1.1 Collab.hq hosted in the IIS data centre

Many investigators and researchers need the capability of Collab.hq as a SaaS product. Collab.hq can be securely accessed in the IIS cloud. The IIS cloud runs in UK data centres in ISO 27001 and PASF approved sites, the locations of which are strictly confidential and only disclosed to client organisations on a need-to-know basis. Our staff are accredited through various schemes as required, for example the Cloud Security Knowledge (CCSK) by the Cloud Security Alliance. All staff are vetted to levels appropriate to their role, with a minimum requirement of NPPV Level 3 with Security Clearance. Where necessary for specific duties, some staff are further vetted to Developed Vetting (DV) level.

Users can triage video and audio files by translating (Collab.trl), transcribing (Collab.tcb) and detecting objects (Collab.obj). These can be files uploaded, such as mobile/laptop downloads, or content held within a user's machine or network. Results can be exported for further analysis and human verification,

saving huge amounts time and money. In an ever-expanding area of intelligence and evidence gathering, many organisations struggle with timely resolutions to tasks of this nature either due to capacity or capabilities internally. This reliance on external assistance, adds further time and cost to an already delayed process so the triage capabilities of Collab.hq are vital. Further models, including text-to-text and OCR are being added the Collab.hq, and more models will be developed in line with user requirements.

The tools can be used together or independently to both transcribe and translate audio to text from large videos and audio datasets using deep learning. New features will be made available via Collab.hq automatically for users to access, using credits to access the features relevant to their role.

The Collab Credits, provide a flexible way for users and organisations to use the full array of AI tools within Collab.hq. Credits can be allocated per user and then utilise when running any of the AI models available through Collab.hq. Depending on the size(s) of the file being analysed, and the model used, the credits will be taken from the available balance. Credits are purchased in bundles and distributed internally by the organisation's administrators.

See Pricing Document for the costs for Collab.hq hosted in IIS data centre.

2.1.2 Collab.hq on prem

There are organisations that require on premise AI for security or integration purposes. IIS will support the implementation of Collab.hq on premise and can provide minimum required specifications for hosting and storage. IIS will provide a full managed service for Collab.hq on-premise along with future upgrades and new models if required by the customer.

Collab.hq on premise does not require credits.

See Pricing Document for the costs for Collab.hq on prem.

2.2 Communicaite™

2.2.1 Communicaite Named User Licence

Communicaite is a secure and standalone translation and transcription product, designed to support law enforcement and secure government organisations. Deployed on both laptop and mobile devices, Communicaite can work online and off-line, dependant on the operational need, and can either produce translations/transcriptions of uploaded content, such as audio and video files, or speech collected directly from the devices microphone. Communicaite also has OCR and text to text translation capability.

The models deployed, are securely hosted within the device and are isolated from the internet, ensuring they are not being trained by the data they access. Communicaite can be deployed on customer devices, as long as these meet certain minimum requirements. Communicaite is fully audited, ensuring compliance at both user and organisational levels.

As future developments become available, updates can be provided to customers' devices.

Communicaite can run connected to our secure cloud or in offline mode.

See Pricing Document for the costs for the Communicaite Laptop and Mobile Access Software Licences.

3. Professional Services

3.1 Training

Our sister company, Vestigo Consulting Ltd, holds exclusive rights to provide IIS product training. This training is not available through any other provider or contractor. Training services can be purchased either directly through IIS or via Vestigo Consulting Ltd.

3.2 Software Support and Maintenance

Where a customer is purchasing licences above the Tier 1 quantities (Collab.hq: first 50; Communicait laptop: first 5; Communicait mobile: first 10), software support and maintenance is included at no additional cost.

Where a customer purchases less than the maximum Tier 1 quantity (Collab.hq: first 50; Communicait laptop: first 5; Communicait mobile: first 10):

- An annual software support and maintenance fee applies, equal to 20% of the licence cost, and
- Onboarding is chargeable and priced separately.

3.3 Hardware Support and Maintenance

Hardware Support is the ongoing maintenance and assistance provided for the firewall throughout its manufacturer-supported lifecycle.

3.4 Onboarding and Tenancy Setup

Where a customer is purchasing licences above the Tier 1 quantities (Collab.hq: first 50; Communicait laptop: first 5; Communicait mobile: first 10), onboarding is included at no additional cost.

Where a customer purchases less than the maximum Tier 1 quantity, a one-off onboarding fee applies.

If a single customer requires further separation between teams, a sub tenancy can be created to silo audit data, views and access between sub-tenancies.

Applicable onboarding and integration costs and options are detailed in the Pricing Document.

4. Onboarding and Offboarding Requirements

4.1 Customer Onboarding

The onboarding process consists of the following steps:

- Contract Execution - The Customer and Supplier must sign the Call-Off Contract to initiate the onboarding process.
- Purchase Order Submission - The Customer must issue a Purchase Order and send it to accounts@ii-solutions.co.uk
- Project Kick-Off Meeting - An initial kick-off meeting will be scheduled between the Customer and the Supplier's Account Manager to review the onboarding plan and key milestones. The Supplier's Account Manager will work closely with the customer throughout the onboarding process to ensure a smooth and supported experience.

- Technical Onboarding Session - A dedicated meeting between the respective technical teams will take place to confirm all technical requirements and configuration details. The Supplier's Account Manager will continue to provide guidance and support during this stage.
- Licence Delivery – The customer will supply user details for those receiving a licence. All licence details, including username and passwords, will be delivered electronically direct to the users once the required steps above are completed.
- Training Arrangements (If Applicable) - If official training has been purchased, the Buyer must book sessions by contacting vestigo@ii-solutions.co.uk with support from the Supplier's Account Manager as needed.

4.2 Customer Offboarding

Upon termination or expiration of an Agreement, the offboarding process will proceed as follows:

- Cessation of Access – All access and usage rights granted to the Customer under the Agreement shall immediately terminate.
- Outstanding Payments – The Customer shall promptly settle any outstanding amounts due to the Supplier under this Agreement.
- Software Access Removal – The Supplier will revoke the Customer's access and usage rights to the Software within 14 working days. This process includes the permanent deletion of any data stored on the platform. If on-prem the Customer must support the Supplier's access to the infrastructure.
- Data Export – Any evidence stored on the Data Transfer Portal must be exported securely. The Customer may initiate the download of their data directly through the Evidence Portal.
- Audit Log Removal – All Audit Logs associated with the Customer's user base will be securely deleted. Audit Logs are retained for 30 days, after which they are automatically purged from the system.
- Credential Destruction – All user management credentials will be securely deleted or destroyed to prevent unauthorised access.

5. Technical Requirements

Our products are accessed through all major supported versions of Web Browsers, including:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Appropriate internet bandwidth must be available. Internet bandwidth requirements will be determined by the number of concurrent sessions. If required, IIS can provide dedicated connectivity at an additional but highly competitive cost, subject to location.

IIS can provide, manage and support a Commercial Product Assurance (CPA) assured VPN device to sit on the outside of the client organisation's boundary firewall, either within a DMZ or sitting directly on the internet. This device creates a highly secure connection to the IIS Cloud enabling our products to be managed from any networked machine.

6. Security and Data Protection

6.1 Security and Compliance Standards

All products have been independently pen-tested by third parties on behalf of customers. TIG has also been awarded Cyber Essentials and Cyber Essentials Plus accreditations.

Our staff are accredited through various schemes as required, for example the Cloud Security Knowledge (CCSK) by the Cloud Security Alliance.

All staff are vetted to levels appropriate to their role, with a minimum requirement of NPPV Level 3 with Security Clearance. Where necessary for specific duties, some staff are further vetted to Developed Vetting (DV) level.

Our products are protected by secure access controls for authentication of users that follow NCSC guidelines with additional measures in place to protect against brute force and unauthorised access.

IIS data centres are ISO 27001 and PASF approved sites in the UK, the locations of which are strictly confidential and only disclosed to client organisations on a need-to-know basis.

TIG is ISO/IEC 27001 certified. This certification applies to its subsidiaries, including IIS, as part of the group Information Security Management System.

Our products are fully compliant with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). Data Encryption is enforced to secure both data in-transit, and at rest.

6.2 Backup / Restore and Disaster Recovery

IIS has internal plans, processes and systems in place regarding business continuity and resilience.

Any specific requirements for backup, restoration and disaster recovery, where appropriate, would be discussed and agreed with the customer prior to an order being placed.

7. Support and Maintenance

Support and Maintenance applies exclusively to IIS products, including Collab.hq and Communicait and any associated IIS solutions. IIS provides comprehensive UK-based Service Desk support during standard business hours via phone and email, working in partnership with the customer's technical team. Alternative arrangements can be agreed upon request.

Incident Management

Faults and requests related solely to IIS products are prioritised under the SLA:

- P1 – Solution down, critical impact; response: 1 working hour, target resolution: 24 hours.
- P2 – Severe degradation; response: 2 working hours, target resolution: 48 hours.
- P3 – Performance degraded; response: 4 working hours, target resolution: 3 working days.
- P4 – Information/admin requests; response: 48 hours, target resolution: 5 working days.

IIS provides 24/7 incident resolution for P1 and P2 affecting IIS products when raised via the correct channels. Out of hours issues are triaged immediately. Collaborative working with the customer's

inhouse teams is required for environment checks, access, and power/network verification. Where that assistance is unavailable, response/resolution times may be impacted.

Availability & Maintenance

Expected availability for IIS products is 99.5%. Planned maintenance for IIS products is scheduled outside business hours and notified 5 days in advance (except for critical security updates). Planned maintenance windows are excluded from availability calculations.

Fault Reporting

Report incidents relating to IIS products via the designated support email. This enables verification (trusted source) and efficient triage. On receipt, a ticket is generated automatically with a reference number and priority confirmation. Urgent tickets should be flagged to the service desk immediately.

8. Customer Accounts and Usage Responsibilities

8.1 Account Setup and Contracting

IIS products are designed to provide tenancy-level segregation for security and audit purposes.

For Collab.hq each customer will be allocated a dedicated tenancy within the Platform, corresponding to a Contracting Authority. In cases where a national or regional unit is established and contracted by a Contracting Authority, it will be configured as a separate tenancy fully isolated from other licences purchased by the Contracting Authority. This ensures complete separation of technical configuration and audit data.

For example, a Regional Unit purchasing licences via one of the Police Forces (the Contracting Authority), will be set up with its own tenancy, distinct from any licences purchased by the Police Force (Contracting Authority).

While customers can collaborate for contracting purposes, each tenancy is managed independently within the system. The volume discount model is applied individually to each customer based on their specific tenancy.

Customers also have the option to create sub-tenancy environments strictly for departmental or audit separation. For example, a PSD Team would have a separate sub-tenancy within a Police Force to the III Team.

Communicait is deployed direct on the laptop or mobile owned by the customer.

8.2 Customer Responsibilities

The customer responsibilities include:

- Ensuring strict adherence to the Acceptable Use requirements. Licences are Named User Licences and must not be shared. Licences may be reassigned if a user changes roles or leaves the organisation.
- Managing the Named User Licence base to ensure compliance with the number of users specified in this order form.
- Providing end-user equipment meeting the agreed minimum standards, including adequate network bandwidth, security certificate installation, email configuration, and firewall access management as needed.
- Deploying the software and the platform shortcuts.

- Coordinating and implementing necessary firewall and routing changes for software integration.
- Allocating staff resources to work with the Supplier at agreed times to facilitate equipment/software installation.
- Owning and managing data.
- Ensuring the confidentiality and security of user logins and passwords, prohibiting any sharing of such credentials.
- Providing adequate training to users for the proper utilisation of the products

8.3 Acceptable Use of Licences

- Each Licence is assigned to a named individual and cannot be shared or used concurrently.
- Licences may only be reassigned if the original user leaves the organisation or changes roles such that they no longer require access to the software. Reassignment is limited to one transfer per licence per year, and the new user must be an active employee with a legitimate business need for the software. This provision is intended to support internal transitions and must not be used to circumvent licensing restrictions.
- Our products are subject to audit, therefore any unauthorised sharing or reassignment may compromise audit integrity and is strictly prohibited.
- **You may not:**
 - Share, rent, lease, or sub-licence the products to any other individual or organisation.
 - Modify, translate, reverse engineer, decompile, disassemble, or create derivative works of our products.
 - Reproduce or redistribute the products in any form without written permission.
 - Use the products outside the scope of your organisation's internal operations or for any purpose other than its intended use.
 - Issue licences to third parties not employed by your organisation without written authorisation from IIS.
 - Conduct training on the products unless specifically licensed to do so.
- Organisations must notify IIS immediately if they become aware of any unauthorised use.
- Unauthorised use may result in licence termination and/or financial liability.

9. Additional Information

9.1 Proof of Concept

For Collab.hq IIS offer a complimentary 30-day trial of the products for up to 5 Users to demonstrate functionality and operational value. For Communicaithe the 30-day trial is for 1 laptop or up to 5 mobile phones. On commencement of the 30-day pre-agreed trial period, the customer will be billed for any additional usage as per the pricing schedule. The User will be required to sign a Trial Licence Agreement prior to the commencement of the trial.

9.2 Ordering and Invoicing Process

Licences are invoiced annually in advance upon order confirmation and are non-refundable. Invoices are issued at the start of the contract term, with payment due within 30 days of the invoice date.

9.3 Accessibility

Our documentation and applicable web-based components of the platform are developed with accessibility in mind. We aim to align our web content and documentation with WCAG 2.2 standards where feasible.

While certain parts of our platform are not web-based and therefore not directly subject to WCAG, we consider accessibility best practices during the design and development of our products.

****End****

Contact us.

Please contact our Contracts Team at:

Email – contracts@ii-solutions.co.uk

Phone – 0344 247 0115