

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.

## Long Arm® and Associated Services

|                                                       |    |
|-------------------------------------------------------|----|
| <b>Table of Contents</b> .....                        |    |
| 1. Introduction.....                                  | 3  |
| 2. Long Arm and Associated Services .....             | 3  |
| 3. Nexus™ Scalable Phone .....                        | 6  |
| 4. Securely Deployed AI Capabilities.....             | 6  |
| 5. Cloud Telephony .....                              | 8  |
| 6. Professional Services.....                         | 8  |
| 7. Cloud Training and Consultancy Services.....       | 9  |
| 8. Onboarding and Offboarding Requirements .....      | 10 |
| 9. Technical Requirements .....                       | 10 |
| 10. Security and Data Protection .....                | 11 |
| 11. Support and Maintenance .....                     | 12 |
| 12. Customer Accounts and Usage Responsibilities..... | 12 |
| 13. Additional Information.....                       | 14 |

# 1. Introduction

## 1.1 Overview of the G-Cloud Service

This document presents Internet Investigation Solution Ltd.'s ("IIS") innovative managed attribution Open-Source Investigation platform, Long Arm®, along with a range of complementary solutions from our sister companies. All conveniently accessible through IIS under one streamlined contract.

For more information on the services we offer please consult our secure website at the following URL: [iis-solutions.co.uk](https://iis-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.

Long Arm® is a registered trademark of The Investigo Group® Ltd.

# 2. Long Arm and Associated Services

## 2.1 Long Arm® Desktop Named User Licence

Long Arm® is a secure, mass-deployable solution for online research and investigations, providing users with a remote desktop environment featuring unrestricted internet access and tools for capturing information with evidential integrity. Designed to ensure transparency and compliance, the platform offers full auditability of user activity aligned with legislative and professional standards. Users connect via their existing hardware through an integrated, encrypted and highly secure VPN, eliminating the need for additional devices and reducing security risks.

The solution delivers managed attribution and an obfuscated digital footprint to enhance operational security, while enabling collaboration across subscribing organisations. Features include deployment management, secure evidence transfer, and configurable reporting for accountability. Long Arm is user-friendly, Windows-based, and supports role-based access levels. Training resources, onboarding support, and live OSINT masterclasses are included to help users maximise capability.

## 2.2 Captis™ and Captis Pro™ – Case Management Named User Licence

Captis, included as part of the standard Long Arm licence, is a user-friendly screen capture and recording tool designed for evidential integrity. Compatible with all browsers and applications within the Long Arm environment, it enables complete session recording and produces files in standard formats such as JPG, PDF, and MPEG4. Features include automatic file naming, encrypted storage, image editing (blurring and pixelation), and hashing for master and working copies, ensuring compliance with evidential standards.

Captis Pro is an optional add-on that enhances reporting and documentation capabilities. It includes web URL logging, contemporaneous note-taking, and the ability to generate bespoke deployment reports and disclosure schedules. Cases can be exported or imported to support collaborative working, such as with the CPS.

Captis Pro is an additional feature for Long Arm available at extra cost.

## **2.3 Mobile Virtual Device (“MVD™”) Named User Licence**

Mobile Virtual Device is an exclusive mobile smart phone emulator within the Long Arm environment, bringing the capabilities of physical mobile devices to the user’s desktop. It enables access to mobile-only applications and functionality not available via web versions of the app, with up to three virtual devices per user that can be geographically located anywhere in the world. A verified app store ensures security by preventing access to harmful apps, while users can create contacts and phone books for operational needs without leaving their desk.

Key benefits include full organisational governance and auditability, reduced cost and maintenance compared to physical devices, and enhanced evidential capture through integration with Captis and Captis Pro. Virtual devices can be relocated to different regions, supporting investigations that require location-based intelligence.

This is an additional feature for Long Arm available at an extra cost.

## **2.4 Mobile Access Named User Licence**

Mobile Access Licences provide access to Long Arm where the choice of connection is via a stand-alone or non-networked device connected to the internet. This is an additional feature for Long Arm available at an extra cost.

## **2.5 Geo™ Selector (Per Named User Licence or Site Licence)**

Geo Selector provides the ability for the user to change their Internet breakout point from pre-configured locations throughout the world. Once a location is selected, the digital footprint associated with the session is configured to match in such a way as to withstand the most intense levels of scrutiny.

This is an additional feature for Long Arm available at an extra cost. The Site Licence is for large organisations that require GEO Selector access for all users.

## **2.6 Reporting Module™ Dashboard inclusive of up to 3 non-Long Arm Audit User Licences**

The Reporting Module Dashboard provides nominated audit users with an intuitive, interactive interface to monitor and analyse user activity across the Long Arm platform. It supports compliance with legislation such as the Human Rights Act 1998 and RIPA 2000 by enabling organisations to verify lawful and ethical use and generate custom weekly or monthly audit reports. These reports are often used to demonstrate investigative methodology and compliance during regulatory inspections by bodies such as HMIC and IPCO.

Additional features include management information reporting to identify underutilisation, training needs, and licence reallocation for cost efficiency. Audit users can create bespoke reports, set alerts and thresholds, and subscribe to scheduled updates via dashboard or email. Access levels are configurable, and proactive monitoring is supported through live session tracking. The Reporting Module Dashboard is an optional add-on to Long Arm, requiring a Reporting End User Licence for each user.

## 2.7 Reporting End User Named User Licence

The Reporting End User Licence stores Reporting Module audit data for six months as standard, with options to extend retention to meet customer requirements. This licence is mandatory for every Long Arm user when the Reporting Module Dashboard is purchased, ensuring full auditability and compliance across the platform. This is an additional feature for Long Arm available at an extra cost.

## 2.8 Non-Long Arm Audit Named User Licence

This licence allows additional non- Long Arm users to access audit functionality within the Reporting Module Dashboard. These users have visibility of Reporting Module audit data only and do not have access to any other features within Long Arm . This is an additional feature for Long Arm available at an extra cost.

## 2.9 Non-Long Arm Administrator Named User Licence

This licence allows non-Long Arm users access to administer access and permissions through the Long Arm Admin Portal. This is an additional feature for Long Arm available at an extra cost.

## 2.10 Long Arm Browser™ Named User Licence

Long Arm Browser is a simple to use, cost-effective, and secure browsing solution that enables users to safely access and operate on the internet from any existing customer device. It provides a highly obfuscated digital footprint to protect operational security and is designed for users who require basic, secure internet research capability without the advanced features of Long Arm Desktop.

Users can capture online content to an evidential standard, including full-screen, regional, and scrolling captures, as well as downloading videos and PDFs. Captures can be securely exported via the Evidence Portal for use within organisational networks. Training is delivered through embedded videos and guidance documents, offering flexibility and reducing the need for dedicated sessions. Long Arm Browser is fully audited and integrates seamlessly with existing Long Arm infrastructure and administration.

## 2.11 Collaboraite™ Named User Licence

A Collaboraite Licence provides advanced data and AI capabilities to accelerate research and investigations, identify operational threats, and enable collaborative working across teams, departments, and regions. It includes Collab.db, Welfare Assist, and access to Collab.hq. a suite of in-house AI tools hosted securely within IIS secure infrastructure.

Collab.db allows users to share and search data live time across their organisation and with other collaborated organisations, reducing duplication and improving efficiency. Squads enable near real-time collaboration on deployments, supporting large-scale operations and shift handovers. Welfare Assist protects investigators from distressing content by shielding pages and muting audio, with full audit oversight for manager support.

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 and is hosted securely within the IIS secure cloud. 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.

This is an optional add-on for Long Arm, available at an extra cost.

## **2.12 Collab.hq™ Credits**

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 utilised 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.

This is an additional feature of Collaboraite available at an extra cost.

## **2.13 V-Sims™**

V-Sims is a virtual sim service that is a direct replacement for pay-as-you-go sim cards required for persona management and account creation. It enables the user to receive text messages directly into the Long Arm platform. One V-Sim equals one phone number. This is an additional feature for Long Arm available at an extra cost.

# **3. Nexus™ Scalable Phone**

The scalable phone is a secure technology solution to reduce the use of physical handsets, in favour of simplifying operations by using a single approved device. The solution allows multiple 'containers / emulated applications' to be present on a single physical mobile device. Each container will have its own allocated number(s) to make/receive calls, send/receive SMS and use selected applications.

To use this service the customer must already be an existing IIS Cloud integrated customer, otherwise additional integration will be required at an additional fee.

# **4. Securely Deployed AI Capabilities**

## **4.1 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.

#### **4.1.1 Collab.hq hosted in the IIS data centre (for Non-Long Arm Users)**

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 utilised 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 (no Long Arm licence).

#### **4.1.2 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-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 Collb.hq on prem.

## **4.2 Communicaite™**

### **4.2.1 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.

## **5. Cloud Telephony**

Our sister company, Voix Telecom Ltd ("Voixtel®") has extensive experience in designing and delivering secure telecommunications solutions focused on safeguarding workforce personnel. We work closely with organisations to configure systems that meet their operational and duty-of-care requirements. We provide a range of solutions to support diverse use cases and specialist applications, and we can develop bespoke features to address modern workforce safety and security related communication challenges. Our virtual telephone numbers are not tied to physical hardware and incorporate intelligent call-handling functionality. This enables calls to be routed efficiently and securely, ensuring individuals are connected to the appropriate person or department while maintaining privacy, safety, and continuity of service.

The service is user controlled through web and app-based applications which allows organisations to have full control over where the phone numbers are routed.

Our focus is on providing targeted solutions for niche applications.

## **6. Professional Services**

### **6.1 Software Support, Maintenance, and Onboarding**

For purchases of 50 or more Long Arm licences, software support, maintenance, and onboarding (including standard integration) are included at no additional cost.

For purchases of fewer than 50 Long Arm licences:



- An annual software support and maintenance fee applies, equal to 20% of the Long Arm licence cost.
- A one-off onboarding fee applies, priced separately.

Where additional separation between teams is required, sub-tenancies can be created to silo audit data, views, and access. Full details of onboarding and integration costs are provided in the Pricing Document.

## 6.2 Hardware Support and Maintenance

Hardware Support is the ongoing maintenance and assistance provided for the firewall throughout its manufacturer-supported lifecycle. Please see our pricing document for further information.

# 7. Cloud Training and Consultancy Services

## 7.1 Cloud Training Services

We can offer a range of training and consultancy services relating to Long Arm and Internet Intelligence & Investigation and OSINT. These services are delivered by our sister company, Vestigo Consulting Ltd which operates exclusively in the law enforcement and secure government agencies.

Vestigo holds the exclusive rights to deliver training on the Long Arm platform and all IIS products. Its team consists of former law enforcement officers and agents, each bringing deep practical experience and specialised expertise in Internet Intelligence, Investigations, and OSINT.

Please see the Pricing Document and <https://www.vestigoconsulting.co.uk> for further details on the training available.

## 7.2 Digital Transformation Consultancy

We have designed our own a set of methodologies delivered by our data, analytics, AI, UX/UI and intelligence/investigation experts that utilise the below capabilities to support your digital transformation and maximise the use, optimisation, and ongoing support of your cloud platforms and software:

- Digital, Data & Analytics Discovery & Transformation Strategy
- Data Fusion/Migration via API, Data Lake, Warehousing & Virtualisation
- Data Visualisation via licensed (PowerBI) & open analytics tools
- Secure-by-design, GDS compliant Application & Product Build
- Data Analytics & Artificial Intelligence (AI) integration with Long Arm & Vestigo®
- Data Science, AI & Automation/RPA
  - Machine Learning (ML), Deep Learning (DL) & Text Analytics including Natural Language Processing (NLP)
  - Specialising in i3, OSINT, consented & open/public data.
  - Human-Centred Design delivering user-experience and user-interface (UX & UI)
- Scrum.inc accredited training, coaching & delivery through Agile Scrum, iterative & waterfall.
- Accredited Design Thinking training, coaching and delivery.

## 8. Onboarding and Offboarding Requirements

### 8.1 Customer Onboarding

The onboarding process consists of the following steps:

- Contract Execution - The Customer and Supplier shall sign the Call-Off Contract to initiate the onboarding process.
- Purchase Order Submission - A Purchase Order should be sent by the Customer to [accounts@ii-solutions.co.uk](mailto: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](mailto:vestigo@ii-solutions.co.uk) with support from the Supplier's Account Manager as needed.

### 8.2 Customer Offboarding

Upon termination or expiration of any Call Off Contract, the offboarding process will proceed as follows:

1. Cessation of Access – All access and usage rights granted to the Customer under the Contract shall immediately terminate.
2. Outstanding Payments – The Customer shall promptly settle any outstanding amounts due to the Supplier.
3. 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.
4. Data Export – Any evidence stored on the Evidence Portal must be exported securely. The Customer may initiate the download of their data directly through the Evidence Portal.
5. 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.
6. Credential Destruction – All user management credentials will be securely deleted or destroyed to prevent unauthorised access.

## 9. Technical Requirements

Our products are accessed using the standard Microsoft Remote Desktop Client (Windows App), available on supported versions of Windows, MacOS, IOS and Android

Supported operating systems include:

- Microsoft Windows
- Apple macOS
- Apple iOS/iPadOS
- Android

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.

## 10. Security and Data Protection

### 10.1 Security and Compliance Standards

All IIS, Vestigo, Collaboraite and Voixtel Products have been independently pen-tested by third parties on behalf of customers. The Investigo Group 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.

### 10.2 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.

## 11. Support and Maintenance

Support and Maintenance applies exclusively to IIS products, including Long Arm 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 in-house 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 Long Arm and other 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.

## 12. Customer Accounts and Usage Responsibilities

### 12.1 Account Setup and Contracting

The Long Arm Platform and all IIS products are designed to provide tenancy-level segregation for security and audit purposes.

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.

## 12.2 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 the Contract.
- 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

## 12.3 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.

## 13. Additional Information

### 13.1 Proof of Concept

IIS offer a complimentary 30-day trial of the Long Arm products for up to 5 Users to demonstrate functionality and operational value. 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.

### 13.2 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.

### 13.3 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](mailto:contracts@ii-solutions.co.uk)

Phone – 0344 247 0115