ORDER FORM

FRAMEWORK AGREEMENT (INSERT REF: 979)

FROM

Contracting Authority/Customer	HMCTS
Address	102 Petty France, London SW1H 9AJ
Invoice Address	Invoices will be sent to Shared services Celtic Springs Business Park PO BOX 767 Newport. NP10 8FZ Copy to be sent to [REDACTED] [REDACTED]
Contact Ref:	Ref:[REDACTED] Name: [REDACTED] e-mail: [REDACTED]
Order Number	*To be quoted on all correspondence relating to this Order.*
Order start Date	20/08/2022
Order Value	£37,250

TO

Supplier:	Tier 1 Asset Management Ltd
Address:	59, Stanley Road Whitefield Manchester M45 8GZ

Contact Details	Name: [REDACTED] Phone: [REDACTED] Email: [REDACTED]

1.	**TERM**

1.1 Effective Date

1.1.1 This Contract shall commence on **20/08/2022.**

1.2 Expiry Date

1.2.1 This Contract shall expire on: 19/02/2023

1.2.1.1 unless extended at the Customer's sole discretion.

1.2.1.2 Completion in accordance with the terms of the Contract, of the Contract Services specified in clause 2 Goods and / or services Requirement

whichever is the earlier, unless terminated earlier pursuant to this Contract

2.	**GOODS AND/OR SERVICES REQUIREMENTS**

2.1 Contract Goods and/or Services Required

The Contract Goods and/or Services required are as set out herein:

Collection of 2,500 iPads and approx. 165 charging cabinets from 165 HMCTS sites nationwide as detailed in Site list – Appendix 1

300 of the iPad that are in good condition shall be collected and returned to HMCTS

Hard drives will be wiped, and certificates issued within 5 working days of devices being collected.

Suppliers will provide proof of devices recycled within 14 days of collection.

Suppliers will ensure that Staff collecting, and wiping devices are SC cleared.

3. PERFORMANCE OF THE CONTRACT SERVICES AND DELIVERABLES

3.1 Implementation Plan and Milestones (including dates for completion)

*The customer requires an implementation plan to be submitted within 14 days of the commencement of the contract.
*Such milestones/key performance indicators below shall be applicable in addition to any milestones/key performance indicators mutually agreed between the parties and set out in the implementation plan.
***Once agreed the Implementation Plan will form part of the contractual documents and failure to meet the milestones/key performance indicators by the stipulated dates may be enforced as a breach of contract.**
***TIME IS OF THE ESSENCE FOR DELIVERY OF THE MILESTONES/KEY PERFORMANCE INDICATORS.**

(i) The Implementation Plan as at the Effective Date is set out below:

[REDACTED]

(ii) If so required by the Customer, the Supplier shall produce a further version of the Implementation Plan (based on the above plan) in such further detail as the Customer may reasonably require. The Supplier shall ensure that each version of the Implementation Plan is subject to approval. The Supplier shall ensure that the Implementation Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation of the Services.

(iii) The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

(iv) The Supplier shall perform its obligations so as to achieve each Milestone by the Milestone Date.

(v) Changes to the Milestones shall only be made in accordance with the variation procedure and provided that the Supplier shall not attempt to postpone any of the Milestones using the variation procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a Milestone by the relevant Milestone Date).

3.2 Performance Monitoring

*****Performance will be monitored by the milestones/key performance indicators set out in the implementation clauses as oulined above.
The Supplier will produce weekly reports for the project team.
At the end of the project, both parties will have a review meeting to ensure the contract has been performed satisfactorily in line with the specification detailed in herein**.**

4. CALL-OFF TERMS AND CONDITIONS

4.1 The YPO 979 framework agreement terms and conditions will apply.

5.	SPECIAL TERMS AND CONDITIONS

5.1 GRANT FUNDING MONIES – N/A

5.2 CLAWBACK: N/A

5.3 DEADLINES: All devices to be collected and disposed as detailed in 3.1 above

5.4 KEY PERFORMANCE INDICATORS: [REDACTED]**.**

5.5 PROVISION OF MANAGEMENT, MONITORING AND REPORTING INFORMATION - N/A
Supplier to certify that all data has been wiped
Supplier shall certify that devices have been disposed in line with ISO 27001:2013 (or its equivalent) standard.

6.	CONFIDENTIAL INFORMATION

Not used

7.	Staff Vetting Procedures

The Staff Vetting Procedures are:

SC cleared, plus Basic Disclosure (Scotland) vetting

Appendix 1 Site List

SITE LIST

[REDACTED]

Appendix 2:

PRICES FOR GOODS AND/OR SERVICES

AS DETAILED IN THE ATTACHED PRICING SCHEDULE

CHARGES FOR SERVICES

Contract Charges

ACTIVITIES	TOTAL COST EXCL VAT
Collection of 2,500 iPads and approx. 165 charging cabinets from 165 HMCTS sites nationwide as detailed in Schedule 1	Secure collection: [REDACTED] iPads and cabinets for recycling: [REDACTED] iPads for re-deployment: [REDACTED] Delivery for re-deployment: [REDACTED] **Total price: £37,250.00 plus VAT.**

Charging mechanism, price and Day Rates	As detailed in the **Pricing Schedule submitted by the Supplier in support of their bid,** The Supplier will submit a valid Invoice for the sum of £37,250 following the completion of the project with required certificates issued.
Invoicing arrangements	On a receipt of a valid Invoice, payment will be made to the Supplier within 30 days of the date of the invoice. If an invoice is disputed it will be returned to the Supplier with details on why the invoice cannot be processed for payment. **Any changes to this standard requirement will need to be set out in the Specification**
Performance-related payment	
Travel and Subsistence	***N/A***

Appendix 3: (Variations and/or supplements to the Call-Off Terms) -Not used

SIGNATORY PAGE:

BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES to enter a legally binding contract with the Customer to provide to the Customer the Goods and/or Services specified in this Order Form (together with where completed and applicable, the mini-competition order (additional requirements) set out in this Order Form) incorporating the rights and obligations in the Call-Off Terms and Conditions set out in the Framework Agreement entered into by the Supplier and YPO on 1st Oct 2019.

For and on behalf of the Supplier:

Name and Title	[REDACTED]
Signature	[REDACTED]
Date	[REDACTED]

For and on behalf of the Customer:

Name and Title	[REDACTED]
Signature	[REDACTED]
Date	[REDACTED]

Appendix 4

CALL-OFF TERMS AND CONDITIONS VARIATION FORM

CALL-OFF TERMS AND CONDITIONS FOR GOODS AND/OR SERVICES

[Name of Lot**] ……**

No of Order Form being varied:……

Variation Form No:……

BETWEEN:

[ ] ("**the Customer"**)

and

[Tier 1 Asset Management Ltd.] (**"the Supplier"**)

1. The Order is varied as follows; [list details of the Variation]

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Authorised to sign for and on behalf of the Customer

Signature .....

Date .....

Name in Capitals .....

Address .....

.....

Authorised to sign for and on behalf of the Supplier

Signature .....

Date .....

Name in Capitals .....

Address .....

.....

.....

.....

Appendix 5

KPI

Appendix 6 –
Tier 1

Tier 1- Data Sanitisation Process

1. Secure process

The most wide-ranging and in-depth independent audit that is carried out on Tier 1's premises, processes and evidence-providing capability is undertaken by ADISA (Asset Disposal & Information Security Alliance). The accreditation includes a thorough audit and up to three unannounced audits per year. This provides the peace of mind to customers that Tier 1's process is secure and furthermore ensures compliance with legislation such as GDPR and WEEE thanks to rigorous inspection of contracts and collection paperwork. In turn, this reduces the considerable risk with regard to the related legislative issues associated with secure IT disposal and data integrity at end of an IT asset's life.

Tier 1 hold the highest level of pass at the ADISA standard (Distinction with Honours) and have passed every single unannounced audit. The standard covers the following areas of our business:

ADISA (Asset Disposal & Information Security Alliance) accreditation

- Re-assessed in June 2020 against a published ADISA standard approved by MoD DIPCOG (The Defence InfoSec Product Co-Operation Group UK) and the ICO.
- Received written confirmation of Pass with Distinction with Honours (95+%). Pass with Distinction with Honours means that every single essential criteria has been met and 95%+ of highly desirable criteria have been met.
- Every subsequent 'unannounced' audit has been passed, enabling us to maintain this highest ADISA status
- The audit and standard covered the following areas, with evidence to be shown where required:

o Module 1: Business credentials
- Business Governance
- Financial stability.
- Insurances held.
- Confirmation of licences, certifications and standards held.
- Health and Safety.
- Integrity of website claims.
- Downstream responsibility.

o Module 2: Secure logistics
- Control of the asset during the transportation process.
- Physical Security of the asset.
- Mitigation of risk throughout the transaction.
- Environmental Capabilities.

o Module 3: Processing facility capability
- Controlling the client engagement.
- Protecting the asset.
- Asset management via the establishment of the chain of custody.
- Deploying the tools for sanitisation which are commensurate to the level of risk.
- Managing the downstream supply chain.

The Areas of Assessment are:

- Pre-Collection Criteria.
- External Physical Security.
- Internal Physical Security.
- Processing capability within IAS 5 compliance.
- Software systems.
- Reporting.
- WEEE / e-waste capability.

a. Pre-collection

Our engagement and process always begin with the requirement for an accurate exchange of information. Documentation between the customer and Tier 1 should clearly identify the number and type of assets for disposal, an agreed process or SLA for disposal, knowledge of any protectively marked material and agreed transfer of custody, where the point is formalised that Tier 1 becomes the designated custodian of the assets and becomes responsible for its control and security.

Customers can book collections using the AMO portal, pre-populated by site details for ease of use. Requests for collection are confirmed within 24 hours and collections can be booked with 48 hours' notice. At the same time as booking the collection, each job can be designated with a reference' number which stays with the collection.

In addition to pre-populated collection address details on AMO, information such as the site contact (plus a reserve), mobile 'phone numbers, plus equipment location and any site access restrictions are also pre-populated both to save time when booking and reduce the risk of a failed collection. This means that only the quantity and type of equipment to be collected needs to be filled in on the easy to use online form.

Tier 1 can be very flexible when organising collections, with timed, AM or PM, out of office hours, weekend and public holiday collections available if required and arranged with suitable notice. If collections less than two working days in advance of the requirement are required, Tier 1 will try to arrange where our logistics partners' schedule allows. Crew details and vehicle registration numbers can also be provided in advance for collection from secure sites.

b. Nationwide secure collection

On arrival at the customer site, the driver will have a copy of the collection paperwork that details the customer collection reference and quantities of each type of asset to be collected. The crew will then:
- report to the nominated 'Point of Contact'
- confirm the contact's identity
- walk the route from equipment to vehicle to identify any obstructions/hazards/security considerations.

The logistics crew undertake all the physical lifting, palletising and wrapping of non-data bearing assets to the high standard required by Tier 1 and our customers. As expected of IT logistics specialists, crews provide all packing and wrapping materials and are trained to package assets securely. Data bearing or items of value are transported in sealable crates with consecutively numbered metal seals. Risk of loss and damage to the equipment will pass to Tier 1 upon collection.

Because Tier 1's emphasis is on re-use, the majority of our secure disposal work takes place at Tier 1's premises. This requires an accredited secure logistics process that without exception includes the following features:

- collection vehicles are monitored by GPS Navman business vehicle tracking system
- minimum of a 2 man crew at all times, with additional manpower provided for larger collections
- vehicles are never left unattended when assets are on board
- drivers and their colleagues have mobile phones
- vehicles have immobilizers operated from the key fob
- vehicles are also fitted with slam locks
- vehicles are fitted with full steel bulkheads preventing access from drivers cab and all load compartment
- doors are also fitted with high security slam locks
- vehicles take the fastest, direct route from the client site to Tier 1 with no unnecessary stops or diversions.
- overnight stops in secure locations will only occur when they are geographically required

There is an emphasis on security and safety inside the cab as well as out. Operationally, the process is controlled by dedicated software that is linked by an advanced data and telecoms network which ensures a seamless transition of information throughout the UK. Drivers maintain an active vigil over both the goods and vehicle. Any anomalies, vehicle problems or concerns are reported immediately to both Tier 1 and logistics operations. The customer would then be contacted directly with the details of any delays or issues. These are backed up by the completion of an Incident Report Form.

In addition, drivers maintain constant communication via mobile phones to escalate on site difficulties or traffic issues to their traffic management office if required.

Imposter prevention is achieved by providing driver IDs to the customer between 48 and 24 hours prior to a collection taking place and drivers carry Government-provided photo ID (eg driving licence, passport) at all times. All logistics and collection crews have licence checks every 3 months and are vetted to SC clearance level. In addition, as part of the collection process, signatures of both the driver and the customer's site contact are required on all paperwork and confirmation of the site contact is made when the vehicle arrives at site.

If an overnight stop at a hub is required:
- goods are offloaded from vehicle to 'goods in transit' secure area of warehouse designated for Tier 1
- goods are never left overnight in the vehicle
- goods will be collected and trunked overnight and delivered next day to Tier 1

As well as regular checks to ensure that our logistics partner has and maintains necessary licences such as waste carriers' licences or hazardous waste carriers licences, we audit our logistics partner's private hub sites to ensure that they incorporate the following security attributes:

- Security Procedures
- Emergency Contacts
- Driver security awareness training
- Access control to Operations Office
- 24/7 Contacts
- Out of hours site control
- Restricted and controlled access to warehousing
- All permanent staff security vetted

- PCs and electronic data password protected
- Constant monitoring of movements by Operations
- Goods Tracking Procedure incorporating unique referencing system

In a new initiative to add an extra level of security to our collection process, assets will have their asset tags or serial numbers scanned on-site before being placed into sealable crates or palletised. A report of what has been collected is then made available on AMO before the equipment has even reached Tier 1 and can be accessed by the customer on the day of collection.

In addition to the on-site scanning process, an asset list with quantities and equipment type are entered onto the collection paperwork, signed by authorised person and a copy left with the authorised, named person. Details of any extra or unexpected items collected are also entered onto the paperwork, but if specifically required by a pre-agreed SLA, Tier 1 will refuse to collect unauthorised or additional assets.

2. Data integrity and secure erasure

a. Product identification, chain of custody and asset logging

As consignments arrive at Tier 1, crates are counted, seals checked for completeness and that they match the seal numbers noted on the paperwork. Quantities of each asset type are checked against both the consignment paperwork signed off by the courier and client site contact at the point of collection and the on-site scanned information provided to Tier 1 prior to arrival.

Consignment checking takes place within 24 hours of delivery to Tier 1. Any discrepancies are first verified by a warehouse supervisor and reported immediately to the Operations Manager or Service Delivery Manager for resolution. Similarly, poorly packed or damaged goods are reported and we take digital photographs as evidence, even if the consignment has been delivered to us.

Within 48 hours, every single item of equipment is logged on to AMO, Tier 1's management information system, double bar-coded to ensure full traceability and these remain with the asset throughout its life at Tier 1. AMO is a comprehensive, bespoke database that allows for real time tracking and asset management of all

equipment from the moment it is received and the services carried out on it, to its eventual destination, be that resale, re-use, or recycling.

This process generates an automated ‘audit report’. This is uploaded onto AMO to verify the items that have been collected and booked in within 2 days of arrival at Tier 1:

a) collection ID
b) Tier 1 unique bar code number
c) type of asset
d) manufacturer
e) model
f) part number
g) serial number
h) asset number

Tier 1 can trace a data-bearing asset from the moment it is collected on site, through the services carried out, to its eventual destination, be that resale, re-use, redeployment, or recycling. Real time asset management and traceability are provided. Tier 1 will maintain adequate indemnity insurance against all risks of loss or damage to stock arising from a fortuitous event unless otherwise excluded from the insurance policy. This cover shall apply to all assets from collection at a client’s site, until the point at which they are resold or environmentally disposed of.

Tier 1 has embarked on a program of getting operational staff up to SC level. Currently we have 17 of our operations team cleared to SC level and only these individuals would handle assets containing data. All Tier 1 staff have Basic Disclosure level clearance.

The Tier 1 warehousing and data processing areas are designed to promote a smooth flow of assets throughout our entire process. Using clearly marked signage to indicate each stage in the process, data bearing assets progress down

a clearly marked path separate from non-data bearing assets. Following the data erasure or data destruction process, data safe assets are stored in a bonded warehouse to ensure that there is no chance for data bearing items to be transferred there inadvertently.

One of the major aspects of Tier 1's process that we champion is the quality of our statistical data and its availability to view on AMO at any time. Not only does reporting promote control over the process, but it also demonstrates transparency over the various activities taking place. This openness is essential to help influence perception of our service to show the number of quality stages in Tier 1's truly robust IT asset disposal process. Our secure AMO portal allows the customer to see these reports online.

b. Data integrity and sanitisation.

Following the booking in process, as part of Tier 1's process before an asset undergoes National Cyber Security Centre (NCSC) approved Blancco data erasure, a manual check is undertaken to identify any removable media eg CD, DVD that has been left in an asset. Similarly, laptop bags are also checked for any loose media, but Tier 1 recommends that laptops or PCs are not sent in bags or boxes. If any such media is found, Tier 1 will contact the customer and provide asset information wherever possible of the asset that the removable media was found within.

In addition to checking for removable media, data bearing assets that come to Tier 1 are physically checked for the presence of more than one HDD. A QA sticker is applied to the machine to confirm that this has been carried out. Extra HDDs are removed and data wiped or destroyed, according to the agreed SLA. All media devices are checked and media is shredded at Tier 1. A second QA sticker is applied to the machine to confirm the device has been checked.

All assets undergo 3 level Higher level data erasure using the latest NCSC approved Blancco software. An IAS 5 recommended data sanitisation process is used for data bearing assets with no magnetic hard drive. Our standard policy for SSD drives is also to overwrite using Blancco. If the customer do not agree to this, SSD drives are physically destroyed to CPNI standards, but customers should be aware that this could affect commercial agreements.

In addition, assets are given a functionality test, engineering and repair (if viable), professional refurbishment, final quality testing, cosmetic grading and high-quality packaging for re-sale. Where items cannot be re-used, they are harvested for parts to be used in other repairs or refurbishment.

All items have a certificate of secure disposal, data erasure or data destruction. At this stage, a Test Report which includes the Blancco data erasure certificate number is provided.

Following completion of the data wiping process, each asset will be labelled with a QA sticker. A second SC cleared Tier 1 employee carries out a data wipe check, confirms all asset labels or tags have been removed and a final QA sticker is added to the asset. A Test Report is then provided to cover the following areas: full item specification, assessment, services carried out, fitness for use and full data erasure certificate.

Where data bearing media takes the form of CD/DVD, memory sticks, tape or HDDs that cannot be overwritten due to having bad sectors or being faulty, physical destruction takes place. These items will be shredded and recycled
in accordance with the WEEE legislation and within CPNI conditions. A certificate of destruction and compliance will be available for every HDD sanitised by Tier 1.

In circumstances where a hard disk drive is inoperable or has bad sectors and can therefore not be guaranteed to have data sanitised using Blancco Data Cleaner:

-hard disks would be removed from machines, re-booked onto the system so that the HDD can be associated with the asset from which it was removed and destroyed within a MOD-approved process.
-the hard disk would be punched and then physically shredded and recycled.

Tier 1 ensures the physical destruction of data and data bearing assets via an approved process, meaning our facilities for the physical destruction of data bearing assets follow an ISO 9000 accredited process, use NCSC approved destruction equipment and is carried out by appropriately security cleared staff.

Hard drives are locked securely until they are shredded to a standard 20mm (or 6mm if required at Higher Level) on site at Tier 1 under cover of CCTV, which can be witnessed via webcam if required.

The IAS 5 process is also adhered to for assets that may not contain magnetic hard drives (such as routers). The process to destroy data on assets such as networking equipment, printers and MFDs depends on the environment where they have come from and the SLAs of the customer. If they have come from HM Government sites, Tier 1 asks the client for the level of security environment the device has come from and this will be clearly marked on the collection paperwork. If required, physical destruction is undertaken, however, if not, then the following is undertaken.

Printers / MFDs: Perform full factory reset to restore factory default settings and print 5 pages of text on each cartridge contained.

Apple products with x86 architecture are overwritten with Blancco software and customers are asked to acknowledge this process where devices are designated for re-use.

Networking equipment: Perform a full manufacturer's reset to rest the device back to its factory default settings. (The same process is followed for non-Government assets). As per all assets handled by Tier 1, each individual asset is booked in, given a barcode and reported as required at the end of the process.

All assets have asset tags or any other identifying markings or labels removed as part of our ISO 9001 process. Where any etching has taken place, this is reported on the Test Report.

Assets will be physically destroyed / shredded to the following IAS 5 Secure Sanitisation Level 1 (Destroy) approved standards:

Device Type	Data Erasure for re-use	Destruction
Hard Drives	NCSC Higher level over-write using Blancco	Shred to 6mm - 20mm maximum
SSD Drives	NCSC Higher level over-write using Blancco – with customer's written permission	Shred to 6mm - 20mm maximum

USB Sticks	n/a	Shred to 6mm - 20mm maximum
LTO Media Drives	n/a	Shred to 6mm - 20mm maximum
DLT Media Drives	n/a	Shred to 6mm - 20mm maximum
DAT/DDS Tapes	n/a	Shred to 2mm - 20mm maximum
Audio Tapes	n/a	Shred to 2mm - 20mm maximum
DVD/CD Media	n/a	Shred to 2mm - 20mm maximum
Mobile phones	Data sanitisation in line with Manufacturer's recommendation plus Blancco Mobile version	Shred to 6mm - 20mm maximum
NV RAM	n/a	Shred to 6mm - 20mm maximum
Hand held & Scanning	Data sanitisation in line with Manufacturer's recommendation	Shred to 6mm - 20mm maximum
Apple products	x86 architecture can be erased with Blancco Erasure Software	Shred to 6mm - 20mm maximum

Following the completion of the data sanitisation process, Tier 1 provides a Test Report to the customer within 10 working days of arrival to document the following information.

The Tier 1 process is designed and tested to ensure that no data bearing assets ever leave the Tier 1 premises. Several checks and balances are in place and are regularly tested as part of both our ISO 27001 and ISO 9001 standards to guarantee that the agreed process is adhered to. We do however understand the requirements of the Information Commissioner when data breaches occur at any level.

Our secure process is designed for us to be able to identify, react to and communicate any unauthorised or accidental deviations from the agreed statement of work. A number of safeguards are in place to prevent any further activity taking place before a resolution to an issue is implemented. The entire process is backed by a thorough and robust adherence to the ISO 9001 standard that has been an established bedrock of Tier 1's business since 2005 and our ISO 27001 standard that covers the entire scope of our organisation, not just the data destruction process.

3. Secure premises and staff

Tier 1’s premises are accredited as HMG ‘List X’ by the MoD. This allows us to handle data bearing assets from the public sector classified as up to and including ‘secret’.

HMG List X site assurance and audit programme

- Assessed with written confirmation of renewal by MoD Industrial Security Advisor (name available on request).
- Approved to hold PMM up to and including SECRET to support current and future projects on a rolling basis, with a revue to be scheduled in 2022.
- The audit covered the following areas with evidence to be shown where required:
  - Company information, business activity, roles and clearance of named individuals
  - Business continuity and contingency plans
  - Personnel, visitor management and training
  - Site security instructions
  - Physical site security, including designated areas for PMM, perimeter security, CCTV, security guards, security lighting and intrusion detection systems
  - Operational requirements
  - Document security
  - IT security

Tier 1 has nearly 40,000 square feet operational facility, including 8,000 square feet of mezzanine flooring dedicated to engineering and Microsoft Approved Refurbishment. The logistical capabilities of our warehouse, investment of new warehouse racking and administrative support mean that Tier 1 has enough capacity to support several thousand further products per month. Our tested and established processes, plus a multi-skilled staff will ensure that additional product will not cause disruption to the smooth running of our organisation.

Tier 1's premises are totally secure and have strict access policies to ensure that they are open only to authorised personnel. In addition, our ISO9001 standard requires us to keep work and storage areas clean

and tidy, minimising the risk of any damage to goods in storage. Staff are trained regularly in handling goods and fork lift truck drivers undergo refresher courses. Cross-training of staff allows us to maintain these standards throughout the warehouse environment.

The standards dictated by our HMG 'List X' status and our ISO 27001 accreditation, whose scope includes all aspects of our business, including secure access and accessibility to systems. The List X approval means that we are approved to hold PMM up to and including SECRET to support current and future projects on a rolling basis.

Within the Tier 1 operations centre, customer assets are protected by a state of the art Chubb Gardtec PR4896 security system. The operations centre has 360-degree surveillance from four external cameras, all constantly monitored by the physical security guard, on VDU's within the security lodge or the remote monitoring station. 48 HD CCTV cameras cover every square foot of the internal building. All real time images are recorded and stored off
site for 31 days. The external of the operations centre is also protected by an infrared security system and as well as all main doors and windows being alarmed, there are sensors located around the building.

Our Redcare alarm is monitored by Visual Verification Ltd. when the on-site security guard is not present and Director and security staff have online access to the cameras.

A physical security guard presence is maintained ten hours a day, five days a week. Outside these hours security is transferred to a remote monitoring station, providing 24 X 7 security cover. Exit from the operations centre is via the security lodge. Without exception, every person leaving the building will be searched. The physical security in operation at Tier 1, has been vetted and approved by Special Branch at part of the accreditation that allows Tier 1 to hold UK government protectively marked information marked as 'confidential' and above.

Visitor access to Tier 1 is strictly monitored. The front door of our building is only accessible to staff who use a regularly changed pass code, otherwise visitors are only allowed access by the security guard. Where a collection is being delivered, the driver should display his identification and they will only gain access when allowed to do so by the security officer. If tradesmen are working on site, they too are required to wear identification and high visibility vests to identify them as non-Tier 1 employees.

Once inside the building, visitors are required to show photo ID, sign in and clearly display a visitor's badge whilst on site. Unless accompanied by authorised staff, visitors are not allowed in the warehouse and data processing area and must always be escorted . Like staff members, visitors' mobile 'phones are not allowed into the warehouse area and are secured in the security office. Visitors are also asked to undergo an electronic search using a security 'wand' or 'pat down', depending on the result of the random search process.

As with all aspects of Tier 1's processes and premises, we are open to audit by customers at any time (on receipt of formal identification) and open ourselves to independent audit through a series of unannounced audits by ADISA, who have full access to our building and assets.

Tier 1 recognises that one of the most important problems to manage within our entire security control process is the potential for insider thievery. As part of our List X, ADISA and ISO 27001 audits and assessments, we consider and audit internal security countermeasures, staff checks and controls that mitigate the risk of potential insider theft.

Tier 1 assesses the suitability and competence of potential employees in a number of different ways, namely:
- Job application
- Interview
- Qualifications – vocational and non-vocational
- Assessment tests
- References
- Personal recommendation

Prior to taking up employment with Tier 1, we undergo screening to verify CRB checks, proof of identity using Government provided documents (passport, driving licence), proof of address, proof of ability to work in the UK.

Furthermore, all staff are cleared to Basic Disclosure (Scotland) level and 27 Tier 1 staff, including those working with protectively marked assets are SC cleared.

4. Reporting, management information and KPIs

Tier 1's understanding of the value of accurate and timely data to our customers is well known. As such, this element of our service has formed the basis of the emphasis on continuous improvement, allied to the improvements made to our internal process and service.

The result has been that the key SLAs of reporting on receipted assets (Audit Report) and reporting on tested assets once they have been processed (Test Report) are not only being met but are being fulfilled in a reduced time scale.

Inspired in part by many customers' 'zero email' policies, Tier 1's Asset Management Online (AMO) portal allows reports, certificates and scanned documents to be viewed online 24/7. Project managers have the option of not having the automated reports emailed to them and opting instead to view them online.

This access to AMO is not only limited to selected personnel on a particular customer account but is also available to wider CMDB teams. Since its inception, the number of customer requests for asset status, Blancco certificates, proof of collection paperwork etc has dropped to almost zero from up to 15 requests per week.

At a most basic level, AMO's functionality allows customers to book collections, receive, view and download reports and monitor the progress of individual collections as they are processed by Tier 1. Constant development has meant individual Blancco certificates will be able to be downloaded from the portal, that were once only available from a manual request.

One of the major aspects of Tier 1's process that we champion is the quality of our statistical data and its availability to view on AMO at any time. Not only does reporting promote control over the process, but it also demonstrates transparency over the various activities taking place. This openness is essential to help influence perception of Tier 1's service to show the number of quality stages in Tier 1's truly robust IT asset disposal process.

For each collection, all equipment is booked in and logged on to AMO, Tier 1's in-house Management Information System (MIS). Each individual asset is bar-coded and the following information entered onto AMO. This process generates an automated 'audit report'. This is uploaded onto AMO to verify the items that have been collected and booked in within 2 days of arrival at Tier 1:

a) collection ID
b) Tier 1 unique bar code number
c) type of asset
d) manufacturer
e) model
f) part number
g) serial number
h) asset number

Tier 1 can trace a data-bearing asset from the moment it is collected on site, through the services carried out, to its eventual destination, be that resale, re-use, redeployment, or recycling. Real time asset management and traceability are provided.

Following the completion of the data sanitisation process, Tier 1 provides a Test Report within 10 working days of arrival to document the following information. As per Audit Reports, these reports will be able to be viewed online via our secure Asset Management Online (AMO) portal or emailed to a specific email address in an .xls format as required. This report contains the following information:

a) collection ID
b) bar code number
c) type of asset
d) manufacturer
e) model
f) part number
g) serial number
h) asset number
i) further specification, including processor type/speed, HDD size, memory size, FDD/CD/DVD, cache, video memory
j) collection location and date
k) Tier 1 grading condition
l) end state (usually on sale, redeployed, donation or recycling, including waste transfer notice number)
m) data wipe level
n) 3 level Blancco Data Cleaner data erasure certificate number, where necessary
o) Waste transfer note, where necessary

All Test Reports give every individual asset an 'end state', usually either 'on sale', 'environmental disposal' or 're-deployment.' As a double check, collections cannot be closed unless every data bearing asset has a Blancco erasure certificate or Waste Transfer Note. For added security, Tier 1 runs an exceptions report that picks up an asset's 'original state' that shows if sanitisation has not taken place. All reports are sent on an automated basis to ensure compliance with the agreed SLA timescale and the final Test Report is sent with a Certificate of Disposal that states all assets have been processed in accordance with the recommendations of IAS 5 and disposed in compliance with WEEE Legislation.

Additionally, AMO allows reports to be easily created on an ad-hoc basis for additional information regarding item specifications, conditions, scrap rates or resale values, broken down by source, type or date range.

Thanks to detail that we record on each asset, Tier 1 can provide a sustainability report to highlight the quantity and type of assets that have been re-used or re-deployed and what weight and type of assets have been recycled. This is a commonly requested report as corporate business requires more and more data about the waste they produce, how sustainable they are and the end state of their WEEE related assets. Tier 1 also provides a breakdown of how assets are recycled, thanks to the 'clean' waste we can produce as part of the prison recycling initiative. With a commitment to zero landfill, Tier 1 can provide a breakdown of how constituent parts are recycled.

Reporting and management information KPIs

Service Deliverable	Service Level Agreement	
Scanned collection data	Availability of signed paperwork and scan log of assets, including any damages	On individual collection basis within one day of receipt from the customer site
Audit Report	Delivery of asset details, including make, model, serial number, asset number	On individual collection basis within two days of receipt at Tier 1's premises
Test Report	Delivery of asset details as per short audit, plus unique asset details, Blancco data erasure evidence and cosmetic grading	On individual collection basis within ten days of production of Audit Report
Account overview	List of all assets held at Tier 1 that have undergone testing and been re-marketed or re-deployed or are being stored.	Sent monthly, quarterly or half yearly, as requested by customer account team.

Tier 1 currently provides the following SLA timescales. Whilst our processes have improved and the ability to check reports on AMO on an automated basis mean that these timescales are reduced on a number of occasions, we feel that adding an extra level of pressure by formalising a reduction would add undue pressure to a smooth-running system that currently works very well for both parties.

Service Deliverable	Service Level Agreement
Collection Booking	
Email acknowledgment of booking request	Same day confirmation of collection date if request is before 12.00pm, next working day if after 12.00pm.
Asset Collection	
Collection made on agreed date	Collection to be made on agreed date between 9am - 5pm, Monday - Friday. AM, PM, timed or weekend collections to be arranged on request.
Receipt of Goods	
Delivery to Tier 1 processing centre within x from collection date	Next working day delivery as standard, same day point to point delivery where geographically possible.
Booking in	Delivery of 'Booking In' report within x from collection date. Booking in report sent within 2 working days of receipt
Audit & Test	
	Delivery or availability of 'Audit Report' or data to specified email address within x from collection Audit Report sent within 2 working days of receipt.
Test Report sent within 10 working days of Audit Report.	
Despatches	
	Acknowledgement of assets picked, packed and ready for shipping according to agreed timescales
	Same day, daily acknowledgement of request to dispatch for re-deployment. Assets picked, packed and dispatched in accordance with agreed quantities.

Tier 1 accreditation and industry membership

- 2019 Queen's Award for Innovation winner
- HM Government IA Standard No. 5 – the latest Government approved data security standard
- ISO 9001 Quality Management Standard. Certificate number FS517045
- ISO 27001 Information Security Standard. Certificate number IS 564833
- ISO 14001 Environmental Management Standard. Certificate number EMS 86615
- ADISA (Asset disposal and information security alliance) Fully Accredited business (Distinction with Honours) to DIPCOG approved secure disposal standard.
- ADISA (Asset disposal and information security alliance) Advisory Board member
- HMG 'Greening ICT Delivery Group (GDU) Re-use and Disposal Working Group industry member
- PASF police approved premises
- Blancco 'Gold' partner
- 2018 ADISA 'Best ITAD ' project winner - "Creating genuine social value through secure IT disposal."

- Data Controller, Registration Number: Z4578499