

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SPI-15	SVC Catalogue Audit	Accuracy of the Request Catalogue repository as determined by a spot check of catalogue items	$= (A/B) \times 100$ A. The number of items in the Request Catalogue deemed to be accurate during a spot check. B. The total number of items in the Request Catalogue checked during a spot check	Monthly	≥95%	No
SPI-16	IDAM Service	The percentage of instances where password resets made by an End User are synchronised to all target systems with the exception of systems within an Authority Cloud Services Provider ICT Environment, within agreed timescales of the request being committed. Where the password resets are relayed only to target systems, then the measure shall be limited to relay only rather than synchronisation.		Monthly	≥99%	No
SPI-17	IDAM Service	The percentage of instances where any change to attribute data is synchronised to all target systems, with the exception of systems within an Authority Cloud Services Provider ICT Environment, within agreed timescales of the change being committed on the originating system. Where the Authority makes bulk changes to attribute data, these changes will be excluded from the measurement of this SPI.		Monthly	≥99%	No
SPI-18	Device log on	The percentage of End User Client Devices allowing the End User to access and use the End User Client Device desktop within one (1) minute of End User authentication.		Monthly	≥95%	No
SPI-19	Updates to Incident Records	Percentage of updates to Incident Records within the Defined Time Frames (below) for the relevant	$= (A/B) \times 100$ A. Aggregate number of Incidents	Monthly	≥95%	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

		<p>Incident Severity Level in a month.</p> <p>Defined Time Frames</p> <ul style="list-style-type: none"> Severity 1 Incidents Records are updated with a report of progress not later than thirty (30) minutes after the Supplier has received notification of the Incident and every thirty (30) minutes thereafter until the Incident has been resolved or the Severity Level has been downgraded. Severity 2 Incidents Records are updated with a report of progress not later than one (1) Hour after the Supplier has received notification of the Incident and every four (4) hours thereafter until the Incident has been resolved or the Severity Level has been downgraded. Severity 3 Incidents Records are updated with a report of progress not later than one (1) Service Day after the Supplier has received notification of the Incident and two (2) Service Days thereafter until the Incident has been resolved or the Severity Level has been downgraded. 	<p>assigned to the Supplier and Resolved during the Measurement Period in question for which all due updates to that Incident's Incident Record were provided within the timeframes set out.</p> <p>B. Aggregate number of Incidents Resolved within the Measurement Period in question.</p>						
SPI-20	Problem Resolution on time	<p>The percentage of all Severity Level 1-3 Problems that are Resolved within the specified time frame for all</p>	<p>= (A/B)*100</p> <p>A. The sum of all Severity 'n' problems</p>	Monthly	≥95%	No			

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

		Severity 1-3 Problems where the Service Desk has identified the analysis and resolution of the Problems is the sole responsibility of the Supplier and where the Supplier does not need to work with any other Suppliers to resolve the Problem	Resolved within the specified timeframe during the Measurement Period. B. The total number of Severity 'n' problems Resolved in the Measurement Period. ▪ Severity 1: 95% resolved within 1 calendar week ▪ Severity 2: 95% resolved within 2 calendar weeks ▪ Severity 3: 95% resolved within 3 calendar weeks			
SPI-21	CMDB Accuracy	The percentage of 50 sample Supplier CMDB item level records which are accurate in all agreed respects. The samples must be taken from different elements of the CMDB each month.	$= (A/B) \times 100$ A. The aggregate number of Supplier CMDB record samples plus actual item samples taken in a Measurement Period that are accurate in all respects B. The aggregate number of Supplier CMDB record samples plus actual item samples taken in a Measurement Period	Monthly	≥98%	No

3. Security Operations Centre (SOC) – KPIs

Frequency of measurement for all the Security related Performance Measures is monthly.

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	KPI Target Performance Level	Publishable Performance Information
SOC-KPI-01	SOC Availability	The Percentage availability for the SOC service	$= (A/B) \times 100$ A. The total time SOC was available B. The total time SOC should be available (24x7x365).	Monthly	≥ 99.99%	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SOC-KPI-02	Security Incident Resolution Time (Severity 1 Security Incident Extensive)	The number of Severity 1 Incidents that are Resolved within the specified timeframe, for all those Severity 1 Security Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other Suppliers and Other Service Providers to resolve the Incident.	$= (A/B) \times 100$ A. The sum of all Severity 1 Security Incidents Resolved within the specified timeframe during the Service Period. B. The total number of Severity 1 Security Incidents Resolved in the Service Period.	Monthly	Severity 1 =100% within 4 Service Hours	No
SOC-KPI-03	Security Incident Resolution Time (Severity 2 Security Incident Significant)	The percentage of Severity 2 Security Incidents that are Resolved within the specified timeframe, for all those Severity 2 Security Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other Suppliers and Other Service Providers to resolve the Security Incident.	$= (A/B) \times 100$ A. The sum of all Severity 2 Security Incidents Resolved within the specified timeframe during the Service Period. B. The total number of Severity 2 Security Incidents Resolved in the Service Period.	Monthly	$\geq 95\%$ within 8 Service Hours	No
SOC-KPI-04	Security Incident Response (Severity 1 Security Incident Extensive)	The Percentage of Severity 1 Security Incidents during the Measurement Period that are responded to within 15 minutes from the identification within the SOC's internal monitoring system, to the point of issuing a ticket within the ITSM Product Or within the same timeframe from the Service Desk allocating the Ticket to the security team and the Security teams first update to the Security Incident Record.	$= (A/B) \times 100$ A. The total number of Security 1 Security Incidents responded to within 15 mins from identification. B. The total number of Security 1 Security Incidents identified within the SOC's internal monitoring systems	Monthly	100% within 10 minutes	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SOC-KPI-05	Security Incident Response (Severity 2 Security Incident Significant)	The percentage of Severity 2 Security Incidents during the Measurement Period that are responded to within 30 minutes from the identification within the SOC's internal monitoring system, to the point of issuing a ticket within the ITSM Product. Or within the same timeframe from the Service Desk allocating the Ticket to the security team and the Security teams first update to the Security Incident Record	$= (A/B) \times 100$ <p>A. The total number of Severity 2 Security Incidents responded within 30 mins from identification.</p> <p>B. The total number of P2 Security Incidents identified within the SOC's internal monitoring systems</p>	Monthly	$\geq 95\%$ within 30 minutes (from identification within the SOC's internal monitoring system to issuing a ticket within the ITSM Product)	No
SOC-KPI-06	Security Incident Response (Severity 3 Security Incident Moderate)	The percentage of Severity 3 Security Incidents during the Measurement Period that are responded to within 60 minutes from the identification within the SOC's internal monitoring system, to the point of issuing a ticket within the ITSM Product. Or within the same timeframe from the Service Desk allocating the Ticket to the security team and the Security teams first update to the Security Incident Record	$= (A/B) \times 100$ <p>A. The total number of Severity 3 Security Incidents responded within 60 mins from identification.</p> <p>B. The total number of Severity 3 Incidents identified within the SOC's internal monitoring systems</p>	Monthly	$\geq 98\%$ within 60 minutes (from identification within the SOC's internal monitoring system to issuing a ticket within the ITSM Product)	No
SOC-KPI-08	Security Incident Resolution Time (Severity 3 Security Incident Moderate)	The percentage of Severity 3 Security Incidents that are Resolved within the specified timeframe, for all those Severity 3 Security Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other Suppliers and	$= (A/B) \times 100$ <p>A. The sum of all Severity 3 Security Incidents Resolved within the specified timeframe during the Service Period.</p> <p>B. The total number of Severity 3 Security Incidents Resolved in the Service Period</p>	Monthly	$\geq 98\%$ within 40 Support Hours	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

		Other Service Providers to resolve the Security Incident.				
SOC-KPI-9	Vulnerability Management Scan Coverage	The percentage of Authority Assets in the estate successfully scanned	= (A/B)*100 A. The total number of Authority Assets scanned in a 24-hour period B. The total number of Authority Assets agreed to be in the estate that need to be scanned	Monthly	≥95% within period	No
SOC-KPI-10	Alert Acknowledgement	The percentage of alerts acknowledged during the Measurement Period within 20 minutes of the alert being received	= (A/B)*100 A. The total number of alerts acknowledged within 20 minutes B. The total number of alerts received	Monthly	≥97% within 20 mins	No
SOC-KPI-11	Alert Categorisation	The percentage of alerts categorised during the Measurement Period within 60 minutes of the alert being received	= (A/B)*100 A. The total number of alerts categorised within 60 minutes B. The total number of alerts received	Monthly	≥97% within 60 mins	No
SOC-KPI-12	Vulnerability Management Data Currency	The percentage of data points within the Vulnerability Assessment Record file that are more than 35 calendar days old without review	= (A/B)*100 A. The total number of data points in the vulnerability assessment Record file that are more than 35 days old without review B. The total number data points in the vulnerability assessment Record file	Monthly	≤ 5%	No
SOC-KPI-13	Vulnerability Management	(The number of identified vulnerabilities notified to Authority with the Measurement Period / the total number of identified vulnerabilities within the Measurement Period) * 100	= (A/B)*100 A. The total number of alerts categorised within 60 minutes B. The total number of alerts received	Monthly	≥99% of critical and high within scan period	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SOC-KPI-15	Threat Intelligence	Threats deemed Critical will be notified to Authority within 1 Working Day, and an alert created in the SIEM in 5 Working Days or less dependent on the complexity of the alert to be created	$= (A/B) \times 100$ <p>A. Number of Critical threats identified and notified to the Authority within 1 Working Day from identification and an alert created in the SIEM within 5 Working Days in the service period</p> <p>B. Total number of Critical threats identified in the service period.</p>	Monthly	$\geq 99\%$ within the service period	No
------------	---------------------	---	---	---------	---------------------------------------	----

4. Security Operations Centre (SOC) – SPIs

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	SPI Target Performance Level	Publishable Performance Information
SOC-SPI-01	Respond to Contract Change Requests to the Services	<p>Percentage of Contract Change Requests to the Supplier by the Authority that have a quote completed and returned to the Authority that are capable of acceptance by the Authority, within the allotted key performance indicator for the size/category of change.</p> <ul style="list-style-type: none"> - Small Works – 3 Working Days - Repeatable – 3 Working Days - Project – 10 Working Days (with ROM within 5 Days) - Large Project – 20 Working Days (with ROM within 10 Days) 	$= (A/B) \times 100$ <p>A. The number of change requests by category that are returned to the Authority that are capable of acceptance within their target times</p> <p>B. The total number of requests by category</p>	Monthly	$\geq 98\%$	No
SOC-SPI-02	Percentage of Knowledge Articles updated within agreed timescales	Percentage of Knowledge Articles updated within 24 Support Hours, where an update or change has been identified by any Party and reported to the Supplier.	$= (A/B) \times 100$ <p>A. The number of KA updated within 24 Support Hours</p> <p>B. The total number of KA requiring an update.</p>	Monthly	100%	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SOC-SPI-03	Failed Changes	To monitor and report on the number of requests relating to Operational Changes which are scheduled for implementation by the Supplier, but which are cancelled, failed and/or backed out.	$= (A/B) * 100$ A. The number of scheduled Operational Changes backed out in a month. B. The total number of scheduled Operational Changes in the relevant month.	Monthly	$\leq 5\%$	No
SOC-SPI-04	Open Problems older than 2 weeks	Percentage of open problems that are over 2 weeks old and are not awaiting an action or dependency on another Supplier or the Authority.	$= (A/B) * 100$ A. The number of open problems that are over 2 weeks old and not dependent on another Supplier or the Authority. B. The total number of open problems that are not dependent on another Supplier or the Authority.	Monthly	$\leq 10\%$	No
SOC-SPI-05	Open Problems older than 3 months	Percentage of open problems that are over 3 months old and are not awaiting an action or dependency on another Supplier or the Authority.	$= (A/B) * 100$ A. The number of open problems that are over 3 months old and not dependent on another Supplier or the Authority. B. The total number of open problems that are not dependent on another Supplier or the Authority.	Monthly	0%	No
SOC-SPI-06	Security Incidents	The percentage of Security Incidents that are Resolved within the specified timeframe within the Service Period, for all Security Incidents where the resolution of the incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with any Authority's Other Suppliers and Other Service Providers to resolve the Incident.	$= (A/B) * 100$ A. The total number of all security incidents Resolved within a specified timeframe within the Service Period B. The total number of security incidents Resolved in the Service Period.	Monthly	100%	No
SOC-SPI-07	Reporting and metrics	The percentage of reports that are submitted on or before their due date.	$= (A/B) * 100$ A. The number of reports submitted on time B. The total number of reports that were due to be submitted	Monthly	99% within period	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SOC-SPI-08	Vulnerability Management - Remediation Management and Escalation	Management of reports and escalations in accordance with the agreed reporting and escalation process.	= (A/B)*100 A. The number of reports submitted on time B. The total number of reports that were due to be submitted	Monthly	99% within period	No
SOC-SPI-09	Log source onboarding and tuning	Elapsed time to completion in Working Days from receipt of approved Authority request. Where applicable, the elapsed time excludes time spent waiting for Authority or third parties to complete associated activities.	= (A/B)*100 A. The number of Log onboarding completed on time B. The total number of log onboarding requested	Monthly	95% within 5 days	No
SOC-SPI-10	Use Case creation and implementation	Elapsed time to completion in Working Days from receipt of approved customer request. Where applicable, the elapsed time excludes time spent waiting for Authority or third parties to complete associated activities.	= (A/B)*100 A. The number of Use cases completed on time B. The total number of use cases requested	Monthly	95% within 5 days	No
SOC-SPI-11	Re-opened Severity 3 Security Incidents	Percentage of Severity 3 Security Incidents re-opened or re-logged by End Users within twenty (20) Working Days.	= (A/B)*100 A. The number of Severity 3 Security incidents reopened within 20 Working Days B. The total number of security incidents in the period	Monthly	≤5%	No

5. Network – KPIs

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	KPI Target Performance Level	Publishable Performance Information
NWK-KPI-01	Availability % of NOC	The Percentage availability for the NOC service (ex. Planned maintenance and ITSM Product outages)	= (A/B)*100 A. The total time NOC was available B. The total time NOC should be available (ie 24x7x365)	Monthly	≥ 99.99%	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

NWK-KPI-02	Network Access Availability	A measure of the percentage Availability of network Services within a Measurement Period aggregated across all Authority Premises. Service Credits will be based on the availability of the Active or Active Plus Ports Services across all Authority Premises.	<p>= (B-A)/Bx100</p> <p>A. The actual number of minutes for which the network access was unavailable during the SMP multiplied by the number of End Users affected for each Incident.</p> <p>B. The total number of minutes for which network access was scheduled to be available during the SMP multiplied by the total number of End Users across all Authority Premises.</p>	Monthly	≥99.9%	No
NWK-KPI-03	Network Infrastructure Availability	<p>Percentage availability of network Infrastructure Services within a month. For the avoidance of doubt, this Key Performance Indicator Specification excludes the Network Printers.</p> <p>In measuring performance against this KPI there shall be disregarded from aggregate unavailable hours:</p> <ol style="list-style-type: none"> any outage associated with failures related to hardware and software which is not part of the network Services; the time in any month during a Scheduled Outage; <p>any unavailable hours where the Supplier has not been granted physical access to an affected Site.</p>	<p>= (A-B)/Ax100</p> <p>A. "Scheduled available hours" is the total number of hours within a SMP</p> <p>B. "Aggregate unavailable hours" which is the aggregate number of hours and any minutes of an hour when the network Infrastructure Service was unavailable within a SMP.</p> <p><i>"Unavailable hours" or any minutes of an hour is measured from the time an Incident relating to the unavailability of the network Infrastructure Service is opened either automatically by an automated tool upon its detection or by the Authority or End User reporting it to the Service Desk until the time that the incident is Resolved.</i></p>	Monthly	≥99.9%	No
NWK-KPI-04	Completion of IMACD to time	Percentage of the aggregate IMACDs completed in accordance with the Service Request Management Policies and Procedures within the time periods set out in the Product & Services Catalogue.	<p>= A x 100% B</p> <p>A. The aggregate number of IMACDs completed within the applicable time periods specified in the catalogue within the SMP.</p> <p>B. The aggregate number of IMACDs scheduled to be completed in the SMP</p>	Monthly	≥90%	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

6. Networks – SPIs

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	SPI Target Performance Level	Publishable Performance Information
NWK-SPI-01	Accuracy of Assets	<p>Percentage of Asset Information relating to Assets within the Network Services which is accurate, measured on a quarterly basis.</p> <p><i>Within fifteen (15) Service Days of the first Service Day of each Quarter, the Supplier shall select a sample of one hundred (100) Network Assets to measure the accuracy of the Asset Information held on the Asset Database for those Assets.</i></p> <p><i>For the avoidance of doubt the Supplier shall not select the same sample of Assets to be validated in two consecutive Quarters.</i></p>	$= (A/B) \times 100$ <p>A. The aggregate number of audited Assets within the Network Services where the Asset Information is accurate in the Quarter</p> <p>B. The aggregate number of Assets within the Network Services audited in the Quarter</p> <p>In measuring performance against this Key Performance Indicator, there shall be disregarded any Asset that has been moved, added to, or changed by the Authority where the Authority has not advised the Supplier of such move, add, or change</p>	Monthly	≥98%	No

7. Managed Print – KPIs

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	KPI Target Performance Level	Publishable Performance Information
MP-KPI-01	Print Service Availability	Percentage availability of Network Printer Services within a month.	$A - B \times 100$ <p>A</p> <p>A. "Scheduled available hours" is the total number of hours within a month for all Services described in scope of Network Print Availability</p>	Monthly	≥99%	No

**CONTRACT FOR THE PROVISION OF
IMS4 SERVICES**

MP-KPI-02	Printer Device Vulnerability Patching	Percentage of Print Supplier provided Devices patched for a Vulnerability within the relevant Vulnerability Patch Deployment Time	<p>B. "Aggregate unavailable hours" which is the aggregate number of hours and any minutes of an hour when the Network Print Service was unavailable within such month.</p> <p>"Unavailable hours" or any minutes of an hour is measured from the time an Incident relating to the unavailability of the Network Printer Service is opened either automatically by an automated tool upon its detection or by the Authority or End User reporting it to the Service Desk Service Desk until the time that the incident is Resolved.</p> <p>During the following hours the period of any unavailability of the Network Printer Service shall be reduced by 90% for the purposes of calculating the "aggregate unavailable hours":</p> <p>on a Service Day the hours between 22:00 and 07:00 the next day; and</p> <p>For the avoidance of doubt, any unavailability of the Network Printer Service at a time other than during the times specified above shall be factored into the "aggregate unavailable hours" with no reduction.</p>	Monthly	≥90%	No
MP-KPI-03	Printer System Device	Number of Print Supplier System Devices patched for a Vulnerability within the relevant Vulnerability		Monthly	100%	No

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

	Vulnerability Patching	Patch Deployment Time <i>(Service Credit shall apply for each System Device, within the scope of the Vulnerability Resolution Plan below the Target and in each subsequent Service Period until the SLT is met)</i>				
MP-KPI-04	ITSC Compliance	The percentage of all Supplier service continuity agreed activities executed to intended outcomes - in line with the Service Continuity Plan	$= (A/B) * 100$ <p>A. The number of Supplier outcomes achieved to Authority intended outcome, when a Supplier ITSCM Test event is executed</p> <p>B. The number of Supplier events / outcomes agreed to be in plan to be executed when a Supplier ITSCM Test event is executed</p>	Monthly	≥95%	No
MP-KPI-05	Asset Tracking (Hardware & Software)	<p>Percentage of Asset Information relating to Assets within the Printer Services which is accurate, measured on a quarterly basis.</p> <p>Within fifteen (15) Service Days of the first Service Day of each Quarter, the customer shall select a sample of one hundred (100) Printer Assets to measure the accuracy of the Asset Information held on the Asset Database for those Assets. For the avoidance of doubt the customer shall not select the same sample of Assets to be validated in two consecutive Quarters.</p>	$= (A/B) * 100$ <p>A. The aggregate number of audited Assets within the Printer Services where the Asset Information is accurate in the Quarter</p> <p>B. The aggregate number of Assets within the Printer Services audited in the Quarter</p> <p>In measuring performance against this Performance Indicator, there shall be disregarded any Asset that has been moved, added to, or changed by the Authority where the Authority has not advised the Supplier of such move, add, or change.</p>	Quarterly	≥95%	No
MP-KPI-06	Software Asset	Percentage of individual Software Products managed by the Supplier	$= A/B$	Monthly	≥98%	No

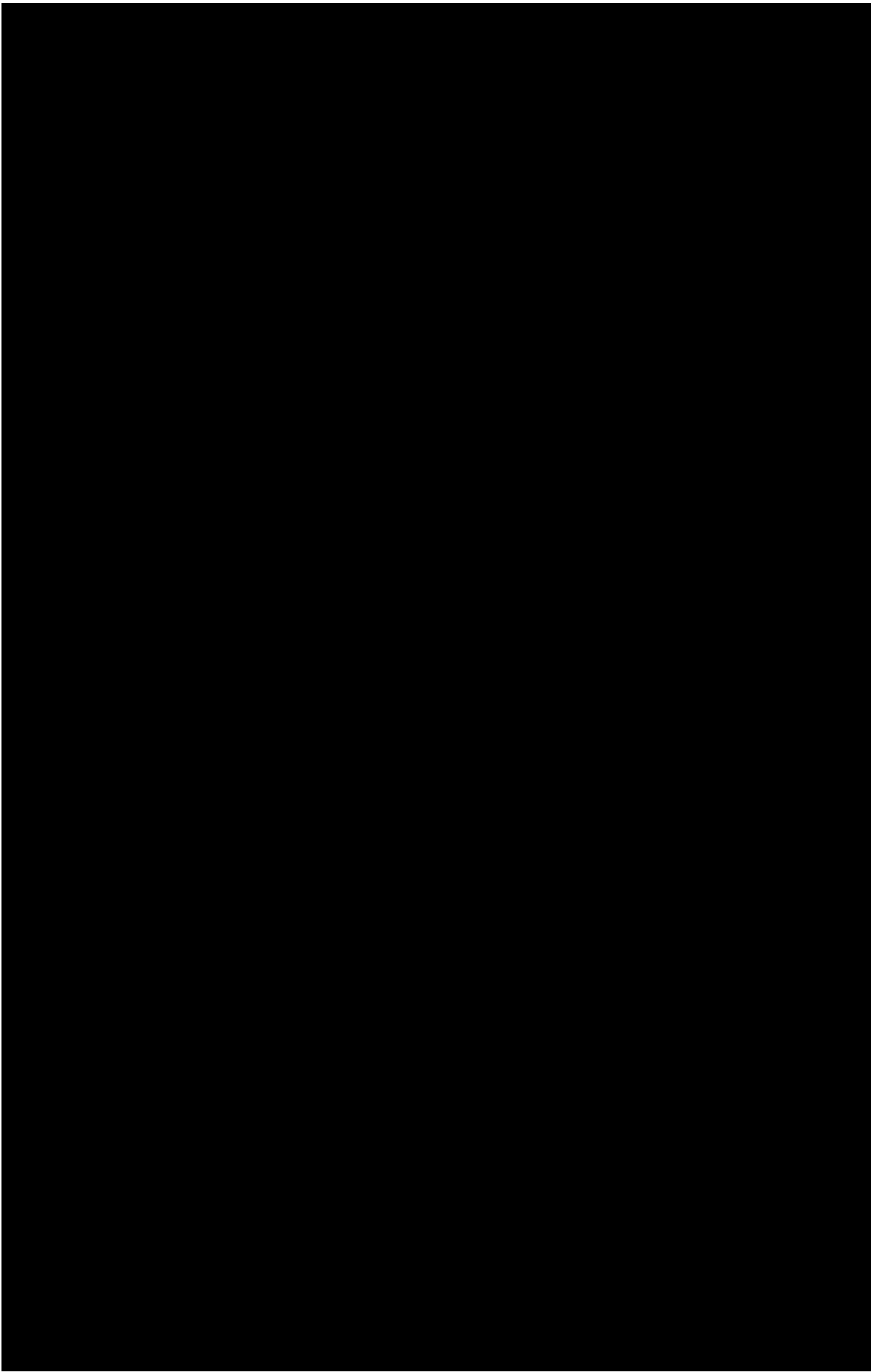
CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

	Compliance	that may incur Authority liability that are compliant through each Measurement Period.	A. The total number of individual software products found to be fully compliant (i.e. the number of instances of that software product were less than the total number of licences purchased by the Authority) in the Measurement Period B. The total number of software products deemed to be the responsibility of the Supplier in the Measurement Period			
--	------------	--	--	--	--	--

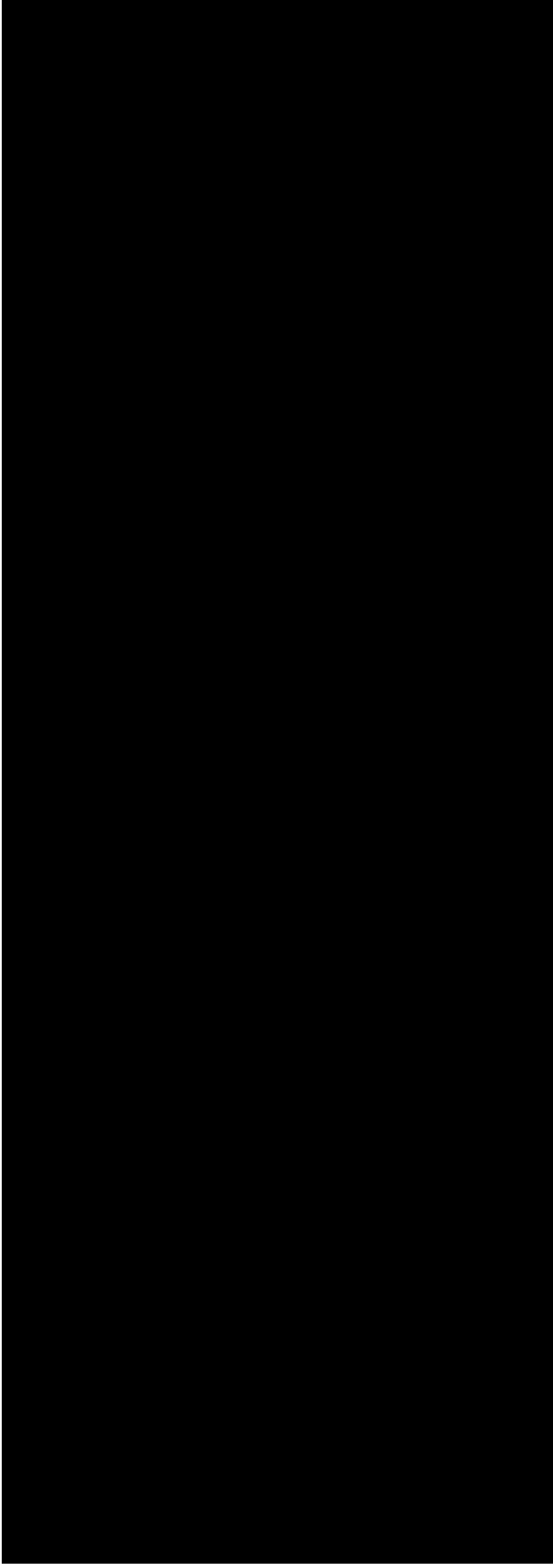
ANNEX 2: STANDARD SERVICE REQUEST CATALOGUE

No.	Description	Key Performance Indicator Target
REQ-01	Password reset	≥ 98% within 5 Service minutes
REQ-02	Create, amend or delete an End User account	≥ 98% within 3 Service Hours
REQ-03	Suspend an End User account	≥ 98% within 30 Service minutes
REQ-04	Create, modify or delete a shared mailbox	≥ 98% within 3 Service Hours
REQ-05	Provide, modify or remove End User access to a shared mailbox	≥ 98% within 2 Service Hours
REQ-06	Create, modify or delete a distribution list	≥ 98% within 3 Service Hours
REQ-07	Provide, modify or remove End User access to a distribution list	≥ 98% within 2 Service Hours
REQ-08	Amend an End User's global address list details	≥ 98% within 2 Service Hours
REQ-09	Deploy or remove Software to (or from) an End User Client Device	≥ 98% within 4 Service Hours
REQ-10	Deploy or remove accessibility Software to (or from) an End User Client Device	≥ 98% within 8 Service Hours
REQ-11	Deploy or remove accessibility hardware	≥ 98% within 4 Service Hours once equipment received
REQ-12	Provide iPhone	≥ 98% within 8 Service Hours
REQ-13	Provide keyboard	≥ 98% within 8 Service Hours
REQ-14	Provide mouse	≥ 98% within 8 Service Hours
REQ-15	Provide headset	≥ 98% within 8 Service Hours
REQ-16	Unblock website	≥ 98% to Security Operations within 2 Service Hours
REQ-17	Printer card request	≥ 98% within 8 Service Hours
REQ-18	International roaming request	≥ 98% within 4 Service Hours
REQ-19	Telephony Group Request (Group Pickup)	≥ 98% within 4 Service Hours
REQ-20	Request, modify or delete Teams site	≥ 98% within 4 Service Hours
REQ-21	Non-Standard request	≥ 98% to Business Engagement within 2 Service Hours

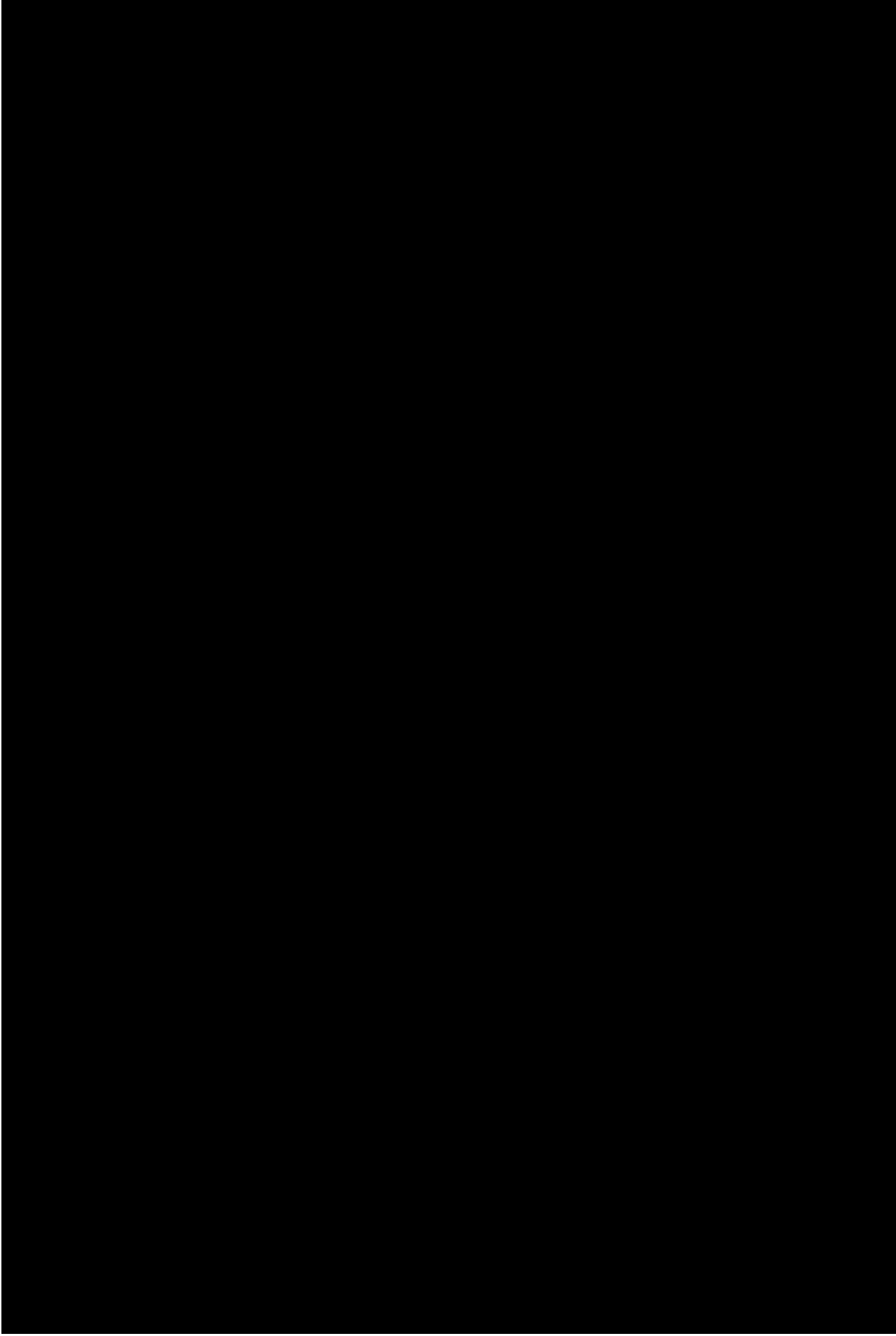
ANNEX 3: SERVICE CREDITS WEIGHTING



CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

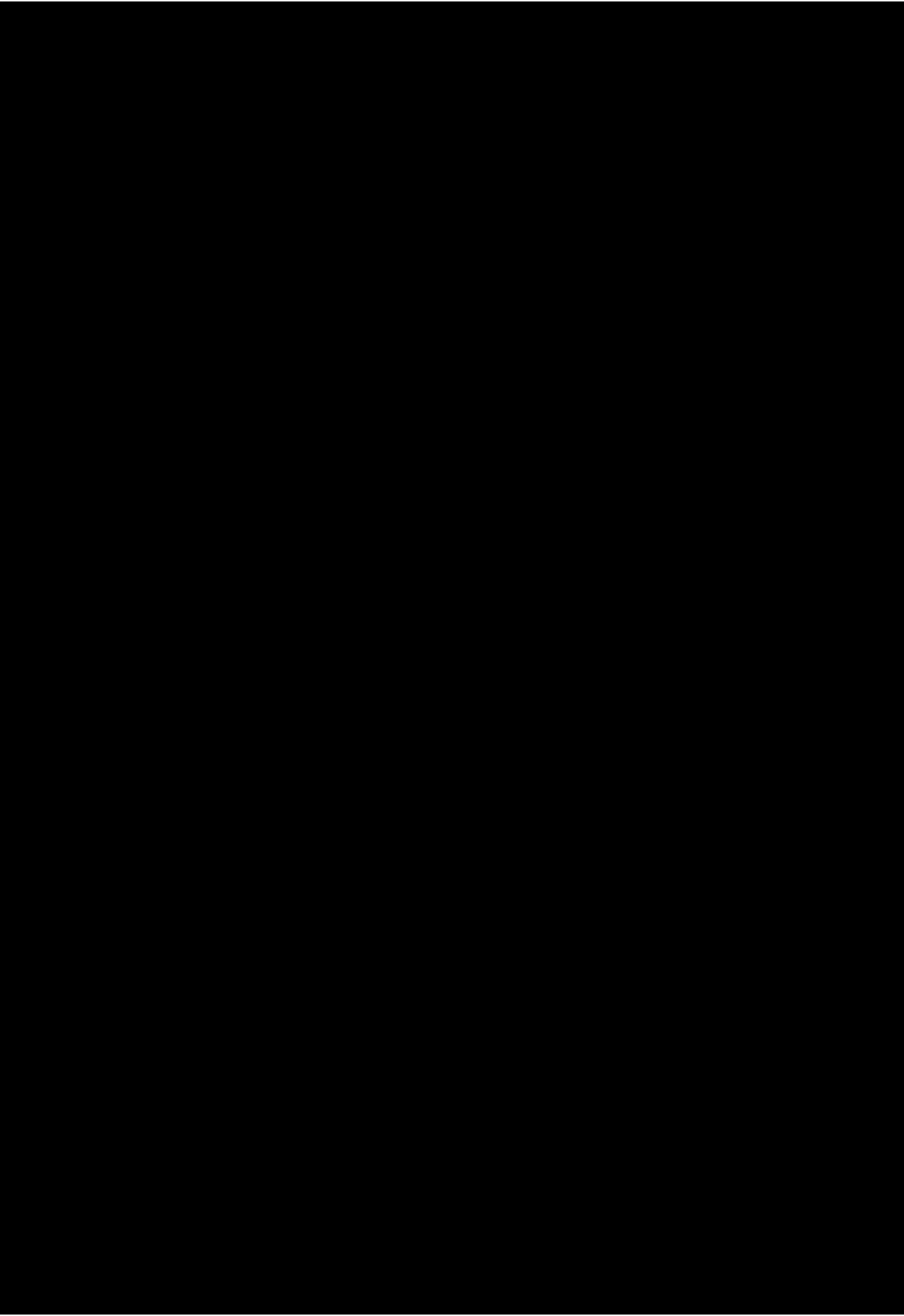


CONTRACT FOR THE PROVISION OF
IMS4 SERVICES



IMS4 – SIGNATURE VERSION

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES



IMS4 – SIGNATURE VERSION

ANNEX 4: TARGET PERFORMANCE LEVELS FOR KPIS CONTRIBUTING TO THE SERVICE IMPROVEMENT FUND

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	Actual KPI Target Performance Level	SIF KPI Target
KPI-01	Service Desk Customer Satisfaction	Service Desk specific customer satisfaction on a scale of 1-5 measuring (a) the delivery and (b) the customer experience. The percentage of respondents to score a total of eight (8) or above on a monthly basis.	$= (A/B) * 100$ A. The number of responses scoring eight (8) or above during a given Supplier customer satisfaction survey initiative. B. The total number of responses received during the given survey initiative period.	Monthly	$\geq 85\%$	The Authority will deem the Supplier delivering exceptional performance when: - all KPIs have met their Target Performance Levels during the relevant Service Period; and - The targets for KPI-01, KPI-02 and KPI-07 are exceeded by 1% or higher; and - The targets for KPI-09 and KPI-11 are exceeded by 0.25% or higher.
KPI-02	First Time Fix (FTF) of Resolvable Calls received by the Service Desk, Tech Hub and Virtual Tech Hub	The percentage of resolvable calls resolved and closed on the first contact by the Service Desk Agent, the Tech Hub or Virtual Tech Hub agent (i.e. Agent does not transfer, escalate change Severity of call or initiate or request a call back).	$= (A/B) * 100$ A. The sum of all resolvable calls received by the Service Desk, the Tech Hub and the Virtual Tech Hub at first contact during the Service Period. B. The sum of all resolvable calls resolved at first contact by the Service Desk, the Tech Hub and the Virtual Tech Hub during the Service Period.	Monthly	$\geq 90\%$	
KPI-07	Incident Resolution Time (Severity 3 Moderate)	The percentage of Severity 3 Incidents that are Resolved within the specified timeframe, for all those Severity 3 Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other Suppliers and Other Service Providers to resolve the Incident.	$= (A/B) * 100$ A. The sum of all Severity 3 Incidents Resolved within the specified timeframe during the Service Period. B. The total number of Severity 3 Incidents Resolved in the Service Period.	Monthly	Severity 3 $\geq 90\%$ within 30 Support Hours	
KPI-09	Service Request Fulfilment	Time to fulfil Service Requests in accordance with the Service Catalogue.	$= (A/B) * 100$ A. The sum of all service requests for which the Supplier is responsible	Monthly	$\geq 99\%$	

CONTRACT FOR THE PROVISION OF IMS4 SERVICES

	KPI- 11	[REDACTED]	The percentage of Service Requests for which the Supplier is responsible which are implemented successfully and within the stated timeframe for that specific request as defined within the relevant Service Catalogue (see Paragraph 7.2 of Part C of this Schedule for individual catalogue item KPIs).	which are implemented successfully and within the stated timeframe for that specific request as defined in the Service Catalogue during the Service Period. B. The sum of all service requests that the Supplier is responsible for implementing during that Service Period.	[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
--	------------	------------	---	---	------------------------------	------------	------------	--

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SCHEDULE 2.3

STANDARDS

SCHEDULE 2.3

STANDARDS

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Standards Hub” the Government's open and transparent standards adoption process as documented at <http://standards.data.gov.uk/>; and

“Suggested Challenge” a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2 GENERAL

2.1 Throughout the Term, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's receipt, of the Goods and Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

2.2 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's receipt, of the Goods and Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

2.3 Subject to Clause 5.4 (*Provision of Goods and Services*), where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

2.4 The Supplier shall comply with the Standards contained in this Schedule, including any successor standards to such Standards that may be published and/or released from time to time.

3 TECHNOLOGY AND DIGITAL SERVICES PRACTICE

The Supplier shall (when designing, implementing and delivering the Goods and Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>.

4 OPEN DATA STANDARDS & STANDARDS HUB

4.1 The Supplier shall comply to the extent within its control with HM Government's Open Standards Principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment, as documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>.

4.2 Without prejudice to the generality of Paragraph 2.2 of this Schedule, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Agreement or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the HM Government's Open Standards Principles (using the process detailed on Standards Hub and documented at <https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology>). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Agreement, an illustration of such requirement

or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

- 4.3 The Supplier shall ensure that all Documentation published on behalf of the Authority pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format Documentation in accordance with the obligation under Paragraph 4.1 of this Schedule to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

5 TECHNOLOGY ARCHITECTURE STANDARDS

The Supplier shall produce full and detailed technical architecture Documentation for the Supplier Solution in accordance with Good Industry Practice. If Documentation exists that complies with The Open Group Architecture Framework (TOGAF) 9.2 or its equivalent, then this shall be deemed acceptable.

6 SECURITY STANDARDS

- 6.1 The Supplier shall comply with all standards (and successor standards) and certification requirements listed in Paragraph 6 of Schedule 2.4 (*Security Management*), including:
- (a) ISO/IEC 27001:2017 Information technology - Security techniques - Information security management systems – Requirements;
 - (b) Cyber Essentials;
 - (c) Cyber Essentials PLUS;
 - (d) Cyber Essentials (for medium-risk contractors) requirements;
 - (e) NCSC Security Design Principles for Digital Services <https://www.ncsc.gov.uk/collection/cyber-security-design-principles;>
 - (f) NCSC Bulk Data Principles <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data;>
 - (g) NCSC Cloud Security Principles <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles;> and
 - (h) any additional standards as may be required in accordance with the Schedule 2.4 (*Security Management*).
- 6.2 The Supplier shall comply with the UK Government Functional Standards GovS007: Security <https://www.gov.uk/government/publications/government-functional-standard-govs-007-security>. This standard applies to government security risk management, planning and response activities for cyber, physical, personnel, technical and Incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm's length bodies or their contracted third parties.
- 6.3 The Supplier shall follow the NCSC guidance on Bring Your Own Device (BYOD) as detailed at: <https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device>
- 6.4 The Supplier shall Apply the government secure email policy as detailed at: <https://www.gov.uk/guidance/securing-government-email>.

7 ACCESSIBLE DIGITAL STANDARDS

- 7.1 The Supplier shall comply with (or with equivalents to):

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- (a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and
- (b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

8 SERVICE MANAGEMENT SOFTWARE & STANDARDS

8.1 Subject to Paragraphs 2 to 4 (inclusive) of this Schedule, the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the provision of Goods and Services, including the following and/or their equivalents:

- (a) ITIL v4;
- (b) ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”;
- (c) ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”;
- (d) ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”;
- (e) ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019; and
- (f) ISO/IEC 23001-14:2019 “Information technology — MPEG systems technologies”.

8.2 For the purposes of management of the provision of the Goods and Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.

9 ENVIRONMENTAL REQUIREMENTS

- 9.1 The Supplier shall comply with the environmental requirements set out in the Annex to this Schedule.
- 9.2 The Supplier shall comply with the requirements of the Greening Government Commitments standards and targets as set out in: (<https://www.gov.uk/government/collections/greening-government-commitments>), including the Greening Government ICT and Digital Services Strategy (<https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025>).
- 9.3 The Supplier shall comply with the EIRs.
- 9.4 The Supplier shall comply with the Waste Electric and Electronic Equipment (WEEE) Regulations 2013.
- 9.5 The Supplier shall work with the Authority to reduce the Authority’s environment footprint.
- 9.6 The Supplier shall (when designing, procuring, implementing and delivering the Goods and Services) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.
- 9.7 The Supplier shall comply with the EU Code of Conduct on Data Centres’ Energy Efficiency.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

The Supplier shall ensure that any data centre used in delivering the Goods and Services are registered as a Participant under such Code of Conduct.

10 HARDWARE SAFETY STANDARDS

- 10.1 The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:
- (a) all hardware required for the delivery of the Goods and Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;
 - (b) all audio, video and similar electronic apparatus required for the delivery of the Goods and Services, shall conform to the following standard: BS EN IEC 62368-1:2020+A11:2020 or any subsequent replacements;
 - (c) all laser printers or scanners using lasers, required for the delivery of the Goods and Services, shall conform to either of the following safety standards: BS EN 60825-1:2014 or any subsequent replacements; and
 - (d) all apparatus for connection to any telecommunication network, and required for the delivery of the Goods and Services, shall conform to the following safety standard: BS EN 62949:2017 or any subsequent replacements.
- 10.2 The Supplier shall perform electrical safety checks in relation to all equipment supplied under this Agreement in accordance with the relevant health and safety regulations.
- 10.3 The Supplier shall follow the UK Government's guidance for service providers who install networking technologies in government shared buildings, known as hub buildings as detailed at: <https://www.gov.uk/guidance/how-to-install-network-infrastructure-in-shared-buildings>.
- 10.4 The Supplier shall follow the UK Government's PSN Guidance and Standards as detailed at: <https://www.gov.uk/government/groups/public-services-network>.
- 10.5 The Supplier shall ensure adherence to the UK Government's Health and Social Care Network (HSCN) standards <https://digital.nhs.uk/services/health-and-social-care-network>.

11 OTHER STANDARDS

The Supplier shall also comply with any additional standards as may be required in accordance with Part A of Schedule 2.1 (*Services Description*) or any other part of this Agreement. In addition, on an annual basis, the Supplier shall discuss with the Authority how the sustainability of the Goods and Services might be improved (including compliance with new or emerging standards relating to sustainability and/or new or emerging government policy requirements relating to sustainability issues).

ANNEX 1: ENVIRONMENTAL REQUIREMENTS

1 DEFINITIONS

1.1 In this Annex, the following definitions shall apply:

Sustainability Reports	written reports to be completed by the Supplier containing the information outlined in Table A of this Annex
Waste Hierarchy	<p>means prioritisation of waste management in the following order of preference:</p> <ul style="list-style-type: none">(a) Prevention – by using less material in design and manufacture. Keeping products for longer;(b) Preparing for re-use – by checking, cleaning, repairing, refurbishing, whole items or spare parts;(c) Recycling – by turning waste into a new substance or produce, including composting if it meets quality protocols;(d) Other Recovery – through anaerobic digestion, incineration with energy recovery, gasification and pyrolysis which produce energy (fuels, heat and power) and materials from waste; some backfilling; and(e) Disposal - Landfill and incineration without energy recovery.

2 ENVIRONMENTAL REQUIREMENTS

- 2.1 The Supplier shall comply in all material respects with all applicable environmental Laws and regulations in force in relation to the Agreement (including the EIRs).
- 2.2 The Supplier shall provide a single point of contact who will work with the Authority's sustainability manager and supply ICT waste data on a quarterly basis, in line with the Authority's Policies and Processes.
- 2.3 The Supplier warrants that it has obtained ISO 14001 certification from an accredited body and shall comply with and maintain certification requirements throughout the Term.
- 2.4 In performing its obligations under the Agreement the Supplier shall to the reasonable satisfaction of the Authority:
- (a) demonstrate low carbon resource efficiency, including minimising the use of resources and responding promptly to the Authority's reasonable questions;
 - (b) prioritise waste management in accordance with the Waste Hierarchy;
 - (c) be responsible for ensuring that any waste generated by the Supplier and sent for recycling, disposal or other recovery as a consequence of this Agreement is taken to an authorised site for treatment or disposal and that the disposal or treatment of waste complies with the Law;
 - (d) ensure that it and any third parties used to undertake recycling disposal or other recovery as a consequence of this Agreement do so in a legally compliant way, and

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

undertake reasonable checks on a regular basis to ensure this;

- (e) inform the Environment Agency within one Working Day in the event that a permit or exemption to carry or send waste generated under this Agreement is revoked and in circumstances where a permit or exemption to carry or send waste generated under this Agreement is revoked the Supplier shall cease to carry or send waste or allow waste to be carried by any Sub-contractor until authorisation is obtained from the Environment Agency;
 - (f) minimise the release of greenhouse gases (including carbon dioxide emissions), air pollutants, volatile organic compounds and other substances damaging to health and the environment; and
 - (g) reduce and minimise carbon emissions by taking into account factors including, but not limited to, the locations from which materials are sourced, the transport of materials, the locations from which the work force are recruited and emissions from offices and on-site equipment.
- 2.5 The Supplier shall use reasonable endeavours to avoid the use of paper and card in carrying out its obligations under this Agreement. Where unavoidable under reasonable endeavours, the Supplier shall ensure that any paper or card deployed in the provision of the Goods and Services consists of one hundred percent (100%) recycled content and used on both sides where feasible to do so.
- 2.6 The Supplier shall complete the Sustainability Report in relation to its provision of the Goods and Services under this Agreement and provide the Sustainability Report to the Authority on the date and frequency outlined in Table A of this Annex.
- 2.7 The Supplier shall comply with reasonable requests by the Authority for information evidencing compliance with the provisions of this Annex within fourteen (14) days of such request, provided that such requests are limited to two per Contract Year.

TABLE A – Sustainability Reports

Report Name	Content of Report	Frequency of Report
Sustainability Impact	<ul style="list-style-type: none"> a. the key sustainability impacts identified; b. sustainability improvements made; c. actions underway or planned to reduce sustainability impacts; d. contributions made to the Authority's sustainability Policies and objectives; e. sustainability Policies, Standards, targets and practices that have been adopted to reduce the environmental impact of the Supplier's operations and evidence of these being actively pursued, indicating arrangements for engagement and achievements. This can also include where positive sustainability impacts have been delivered; and f. risks to the Service and Sub-contractors of climate change and severe weather events such as flooding and extreme temperatures including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks. 	On the anniversary of the Effective Date
Waste Created	By type of material the weight of waste categories by each means of disposal in the Waste Hierarchy with separate figures for disposal by incineration and landfill.	Before contract award and on the anniversary of the Effective Date.
Waste Permits	Copies of relevant permits and exemptions for waste, handling, storage and disposal.	Before the Effective Date, on the anniversary of the Effective Date and within ten (10) Working Days of there is any change or renewal to license or exemption to carry, store or dispose waste
Greenhouse Gas Emissions	<p>Indicate greenhouse gas emissions making use of the use of the most recent conversion guidance set out in '<i>Greenhouse gas reporting – Conversion factors</i>' available online at:</p> <p>https://www.gov.uk/guidance/measuring-and-reporting-environmental-impacts-guidance-for-businesses</p>	On the anniversary of the Effective Date
Water Use	Volume in metres cubed.	On the anniversary of the Effective Date
Energy Use	<p>Separate energy consumption figures for:</p> <ul style="list-style-type: none"> a. assets deployed on the Supplier's premises; b. assets deployed on the Authority's 	On the anniversary of the Effective Date

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

	<p>Premises;</p> <p>c. assets deployed off-site; and</p> <p>d. energy consumed by IT assets and by any cooling devices deployed.</p> <p>Power Usage Effectiveness (PUE) rating for each data centre/server room in accordance with ISO/IEC 31034-2/EN 50600-4-2.</p>	
Transport Use	<p>a. miles travelled by transport and fuel type, for Goods delivered to the Authority's Premises;</p> <p>b. miles travelled by staff when visiting the Authority's Premises from the Supplier's premises or home;</p> <p>c. resulting Green House Gas (GHG) emissions using agreed Conversion Factors; and</p> <p>d. the number of multi-lateral e-meetings i.e. with more than two attendees, held by type (audio, webinar, v/conferencing) their length and number of attendees.</p>	On the anniversary of the Effective Date
Materials	<p>Materials usage, including:</p> <p>a. type of material used;</p> <p>b. quantity or volume of material used; and</p> <p>c. amount of recycled/recovered material used.</p>	

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

SCHEDULE 2.4

SECURITY MANAGEMENT

SCHEDULE 2.4

SECURITY MANAGEMENT

1 DEFINITIONS

1.1 In this Schedule:

“Anti-Malicious Software”	means software that scans for and identifies possible Malicious Software in the IT Environment;
“Breach of Security”	<p>an event that results, or could result, in:</p> <p>(a) any unauthorised access to or use of the Authority Data, the Goods and/or Services and/or the Information Management System, including a loss of (or denial of) access to the same; and/or</p> <p>(b) a Data Loss Event, including the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data and any copies), used by either Party in connection with this Agreement;</p>
“Certification Requirements”	means the information security requirements set out in Paragraph 6 of this Schedule;
“CHECK Service Provider”	means a company which has been certified by the NCSC, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 7.1 of this Schedule;
“CREST Service Provider”	means a company with a SOC Accreditation from CREST International;
“Higher Risk Sub-contractor”	<p>means a Sub-contractor that Processes Authority Data that is considered to be High Risk according to Data Protection Impact Assessment. In particular, a Sub-contractor processing data that includes:</p> <p>(a) Health, Genetic or Biometric data; or</p> <p>(b) other Special Category Personal Data;</p> <p>would be considered a Higher Risk Sub-contractor</p>
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the NCSC;

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

“Incident Process”	Management	means the process which the Supplier shall implement immediately after it becomes aware of an event that impacts the confidentiality, integrity or availability of the Goods and Services, such as a loss of Service or Breach of Security. An incident management process is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Goods and/or Services and/or users of the Goods and/or Services and which shall be prepared by the Supplier in accordance with Paragraph 4.3(c) using the template set out in Annex A 3 of this Schedule;
“Information Assessment”	Assurance	refers to the set of Policies, Procedures, systems and Processes which the Supplier shall implement, maintain and Update in accordance with Paragraph 4 of this Schedule in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Breaches of Security and/or Data Loss Events and which shall be prepared by the Supplier using the first 5 sections of the template Security Management Plan, set out in Annex A 3 of this Schedule;
“Information System”	Management	means <ul style="list-style-type: none"> (a) those parts of the Supplier System, and those of the Sites, that the Supplier or its Sub-contractors will use to provide the parts of the Goods and/or Services (as applicable) that require Processing of Authority Data; and (b) the associated information assets and systems (including organisational structure, controls, Policies, practices, Procedures, Processes and resources);
“Information Approval Statement”	Security	means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the: <ul style="list-style-type: none"> (a) Authority is satisfied that the identified risks have been adequately and appropriately addressed; (b) Authority has accepted the residual risks; and (c) Supplier may use the Information Management System to Process Authority Data;
“IT Health Check”		has the meaning given in Paragraph 7.1(a) of this Schedule;
“Medium contractor”	Risk Sub-	means a Sub-contractor that Processes Authority Data that is not considered to be High Risk according to Data Protection Impact Assessment. In particular, sub-contractors Processing Authority Data that:

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- (a) includes any Personal Data referenced in Schedule 11 (*Processing Personal Data*), in the period between the first Operational Service Commencement Date and the date on which this Agreement terminates in accordance with Clause 4.1(b) (*Term*); and
- (b) does not, at any time, include (or is likely to include) Special Category Personal Data;

would not be considered to be High Risk

“Process”

means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Risk Assessment”

is the risk assessment within the Information Assurance Assessment which is to be prepared and submitted to the Authority for approval in accordance with Paragraph 4 of this Schedule;

“Required Register”

Changes

mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 5.2 of this Schedule together with the date by which such change shall be implemented and the date on which such change was implemented;

“Security Plan”

Management

means the document prepared by the Supplier using the template in Annex A 3 of this Schedule as part of the Implementation Plan, comprising:

- (a) the Information Assurance Assessment;
- (b) the Required Changes Register; and
- (c) the Incident Management Process;

“Special Personal Data”

Category

means the categories of Personal Data set out in article 9(1) of the GDPR;

2 INTRODUCTION

2.1 This Schedule sets out the:

- (a) arrangements the Supplier must implement before, and comply with when, providing the Goods and Services and performing its other obligations under this Agreement to ensure the security of the Authority Data and the Information Management System;
- (b) Certification Requirements applicable to the Supplier and each of those Sub-contractors which Process Authority Data;

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- (c) Baseline Security Requirements in Annex A 1 of this Schedule, with which the Supplier must comply;
- (d) tests which the Supplier shall conduct on the Information Management System during the Term;
- (e) Supplier's obligations to:
 - (i) return or destroy Authority Data on the expiry or earlier termination of this Agreement;
 - (ii) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 9 of this Schedule; and
 - (iii) report Breaches of Security to the Authority.

3 PRINCIPLES OF SECURITY

- 3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:
 - (a) the Authority Premises;
 - (b) the IT Environment;
 - (c) the Information Management System; and
 - (d) the Goods and Services.
- 3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier shall be, and shall always remain , responsible for the security:
 - (a) confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and
 - (b) of the Information Management System.
- 3.3 The Supplier shall:
 - (a) comply with the Baseline Security Requirements in Annex A 1 of this Schedule; and
 - (b) ensure that each Sub-contractor that Processes Authority Data complies with the Security Requirements in Annex A2 of this Schedule.
- 3.4 The Supplier shall provide the Authority with a list of those Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule as part of the Security Management Plan.
- 3.5 The Supplier must assign a designated security contact (DSC) for the provision of Goods and/or Services who will have overall responsibility for compliance with the Supplier's obligations under this Schedule. If the DSC assigned is not at board level alternatively there must be a member of the SIAG to whom representation of the Authority's security implications relating to the provision of this service can be directed. Where deemed appropriate, the Authority may require that the individual (and any other relevant employees) attend agreed security awareness training, which will be at the expense of the Supplier. Where the Supplier deems it relevant, the DSC may assign a single point of contact (SPOC) for the responsibility

of the day-to-day security management, on notice to the Authority in writing. However, the SPOC must report to the DSC and attend all required SIAG meetings.

4 INFORMATION SECURITY APPROVAL STATEMENT

- 4.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule including any requirements imposed on Sub-contractors by Annex A 2 of this Schedule, from the first Operational Service Commencement Date.
- 4.2 The Supplier may not use the Information Management System to Process Authority Data unless and until the:
- (a) Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 7.1 of this Schedule; and
 - (b) Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 4.
- 4.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule and the Agreement in order to ensure the security of the Authority Data and the Information Management System.
- 4.4 The Supplier shall prepare and submit to the Authority within thirty (30) Working Days of the Effective Date, the Security Management Plan, which comprises:
- (a) an Information Assurance Assessment;
 - (b) the Required Changes Register; and
 - (c) the Incident Management Process.
- 4.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within twenty (20) Working Days of receipt and shall either issue the Supplier with:
- (a) an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or
 - (b) a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.
- 4.6 If the Authority rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Authority for review within ten (10) Working Days or such other timescale as agreed with the Authority.
- 4.7 If the Authority issues two or more rejection notices, the failure to receive an Information Security Approval Statement shall constitute a material Default by the Supplier and the Authority may terminate this Agreement with immediate effect as an Emergency Exit by issuing a Termination Notice to the Supplier in accordance with Clause 34.1(c) (*Termination Rights*).
- 4.8 The process set out in Paragraphs 4.3 to 4.6 of this Schedule shall be repeated until the Authority either:
- (a) issues an Information Security Approval Statement to the Supplier under sub-Paragraph 4.5(a) of this Schedule; or

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- (b) terminates this Agreement under Paragraph 4.7 of this Schedule.
- 4.9 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:
- (a) access to the Information Management System; and
 - (b) such other information and/or Documentation that the Authority or its authorised representatives may reasonably require,
- in order to:
- (c) audit and verify the Supplier's and its Sub-contractors' compliance with this Agreement generally; and
 - (d) assist the Authority to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Authority Data and the Information Management System are consistent with the representations in the Security Management Plan.
- 4.10 The Supplier shall provide the access required by the Authority in accordance with Paragraph 4.9 within three (3) Working Days of receipt of such request, except in the case of a Breach of Security (in which case the Supplier shall provide the Authority with the access that it requires within thirty six (36) Service Hours of receipt of such request).

5 COMPLIANCE REVIEWS

- 5.1 The Supplier shall review and Update the Security Management Plan, and provide such to the Authority, at least once each Contract Year and as otherwise required by this Paragraph.
- 5.2 The Supplier shall notify the Authority within two (2) Working Days after becoming aware of:
- (a) a change to the components or architecture of the Information Management System made outside of the Operational Change process described in Paragraph 7.2 of Part A of Schedule 2.1 (*Services Description*) or the Contract Change or Work Requests processes in Schedule 8.2 (*Change Control Procedure*);
 - (b) a new risk to the components or architecture of the Information Management System;
 - (c) a vulnerability to the components or architecture of the Service which is classified 'Critical', 'High', or 'Medium' in accordance with the classification methodology set out in Paragraph 9.2 of Annex A 1 to this Schedule;
 - (d) any change in the threat profile;
 - (e) a change to any risk component;
 - (f) a change in the quantity of Personal Data held within the Information Management System made outside of the Operational Change process described in Paragraph 7.2 of Part A of Schedule 2.1 (*Services Description*) or the Contract Change or Work Requests processes in Schedule 8.2 (*Change Control Procedure*) or outside any applicable obligations of the Supplier under Schedule 11 (*Processing Personal Data*);
 - (g) a proposal to change any of the Sites from which any part of the Goods and/or Services are provided;
 - (h) emerging changes in Good Industry Practice; and/or
 - (i) an ISO27001 audit report produced in connection with the Certification Requirements

indicates any concerns relating to the security controls used to protect the Service.

- 5.3 Within ten (10) Working Days of such notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Authority for review and approval.
- 5.4 Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost and expense.
- 5.5 If the Supplier fails to implement a change set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default by the Supplier which is capable of remedy and the Supplier shall:
- (a) immediately cease using the Information Management System to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to process Authority Data in accordance with the Authority's written directions; and
 - (b) remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Agreement with immediate effect as an Emergency Exit by issuing a Termination Notice to the Supplier in accordance with Clause 34.1(c) (*Termination Rights*).

6 CERTIFICATION REQUIREMENTS

- 6.1 The Supplier shall be certified as compliant with:
- (a) ISO/IEC 27001:2017 by a United Kingdom Accreditation Service- approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2017; and
 - (b) Cyber Essentials PLUS and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.
- 6.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:
- (a) ISO/IEC 27001:2017 by a United Kingdom Accreditation Service- approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2017; or
 - (b) Cyber Essentials PLUS,
- and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.
- 6.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with at least Cyber Essentials.
- 6.4 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:
- (a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2017; and

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- (b) are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.
- 6.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the Certification Requirements before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.
- 6.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier or any Sub-contractor ceases to be compliant with any of the Certification Requirements and, on request from the Authority, shall (or shall procure that the relevant Sub-contractor shall):
- (a) immediately ceases using the Authority Data; and
- (b) procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph 6.
- 6.7 The Authority may (at its discretion) agree in writing to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 6. The Supplier must include the exemption in the Security Management Plan.
- 6.8 The Supplier shall ensure that a cyber assessment and data protection impact assessment has been completed on all of its Third Party Contracts and Third Party Software that are used in connection with this Agreement.

7 SECURITY TESTING

- 7.1 [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- 7.2 [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- 7.3 [REDACTED]
- [REDACTED]
- [REDACTED]
- 7.4 [REDACTED]
- [REDACTED]

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

■ [REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]

7.5 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

7.6 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

7.7 [REDACTED]
[REDACTED]
[REDACTED]

7.8 [REDACTED]
[REDACTED]

7.9 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

8 SECURITY MONITORING AND REPORTING

8.1

- [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]

9 MALICIOUS SOFTWARE

9.1

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

9.2

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

9.3

- [REDACTED]
- [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]

10 BREACH OF SECURITY

10.1

- [REDACTED]
- [REDACTED]

10.2

- [REDACTED]
- [REDACTED]
 - [REDACTED]

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]

10.3 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

10.4 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

ANNEX A 1: BASELINE SECURITY REQUIREMENTS

1 SECURITY CLASSIFICATION OF INFORMATION

If the provision of the Goods and/or Services requires the Supplier to Process Authority Data which is classified, the Supplier will implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards as defined in <https://www.gov.uk/government/publications/government-security-classifications>.

2 END USER DEVICES

- 2.1 The Supplier shall ensure that any Authority Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.
- 2.2 The Supplier shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/collection/end-user-device-security>.

3 NETWORKING

The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

4 PERSONNEL SECURITY

- 4.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Goods and/or Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including verification of the individual's:
 - (a) identity;
 - (b) nationality and immigration status;
 - (c) employment history; and
 - (d) any criminal records.
- 4.2 The Parties shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Goods and/or Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include roles with privileged access (e.g. System Administrators, Domain Administrators) to IT systems which Process Authority Data or data which, if it were Authority Data, would attract a Government security classification.
- 4.3 The Supplier shall not permit Supplier Personnel to be involved in the management and/or provision of the Goods and/or Services prior to completion of the checks required by Paragraphs 4.1 and 4.2 of this Annex A1 and the award in writing of the appropriate National Security Vetting level except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Goods and/or Services.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- 4.4 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 of this Annex A1 to be involved in the management and/or provision of the Goods and/or Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Goods and/or Services.
- 4.5 As required by sub-Clause 24.6(b)(iii)(C) (*Protection of Personal Data*), the Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
- 4.6 The Supplier shall ensure that Supplier Personnel:
- (a) who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within one (1) Working Day; and
 - (b) will have access to the Authority Premises, the IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Authority Premises, the IT Environment or the Authority Data.
- 4.7 The Supplier shall ensure that the training provided to Supplier Personnel under Paragraph 4.7 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Authority Premises, the IT Environment or the Authority Data (“phishing”).
- 4.8 The Supplier shall remove any member of Supplier Personnel without delay from their involvement with the Goods and/or Services, if, in the reasonable opinion of the Authority in writing, any Supplier Personnel engaged in the provision of any part of the Goods and/or Services shall misconduct themselves in such a way that brings the Authority into disrepute, or if it is not in the public interest for such persons to be employed or engaged by the Supplier on any part of the provision of Goods and/or Services. The Supplier shall maintain suitable Procedures in accordance with the Performance Indicators and Schedule 2.2 (*Performance Levels*) to avoid undue dependence on the experience and expertise of individual Supplier Representatives, including the SPOC. Where the SPOC is unavailable at any time, an alternative monitored mailbox shall be provided by the Supplier to receive Service Incidents and Service Requests.
- 4.9 The Supplier shall take all necessary Protective Measures to ensure that all personnel working within close proximity to Supplier Personnel on the provision of any Goods and/or Services at the Authority Premises are always approved to be within any designated area.

5 IDENTITY, AUTHENTICATION AND ACCESS CONTROL

- 5.1 The Supplier shall operate an access control regime to ensure:
- (a) all users of the Supplier Information Management System are uniquely identified and authenticated using Multi-Factor authentication when accessing Authority Data;
 - (b) all administrative access to the Supplier Information Management System are uniquely identified and authenticated using Multi-Factor authentication. Shared Accounts will not be used, and service accounts will be restricted to permissions and privilege needed for the task, and protected with strong, complex passwords.
- 5.2 The Supplier shall apply the ‘principle of least privilege’ and ‘separation of duties’ when allowing persons access to the Supplier System so that such persons are allowed access only to those parts of the Supplier System they require, and authorisation for actions is not consolidated in a single person.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- 5.3 The Supplier shall ensure that all persons who access the Authority Premises where the Service is provided, are identified and authenticated before they are allowed access.
- 5.4 The Supplier shall restrict persons access to Authority Premises so that such persons are allowed access only to those parts of the Authority Premises they require.
- 5.5 The Supplier shall:
- (a) retain records of access to the Authority Premises and to the Supplier System and shall make such record available to the Authority on request;
 - (b) maintain a list of those individual Supplier Representatives' security responsibilities including those responsibilities relating to individuals working on systems supporting its administration (as part of the list required to be provided by Paragraph 3.4 of this Schedule).

6 DATA DESTRUCTION OR DELETION

- 6.1 The Supplier shall:
- (a) prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Authority with all Authority Data in an agreed open format;
 - (b) have documented processes to ensure the availability of Authority Data if the Supplier ceases to trade;
 - (c) securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;
 - (d) securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as agreed by the Authority; and
 - (e) implement processes which address the NCSC guidance on secure sanitisation. <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>

7 AUDIT AND PROTECTIVE MONITORING

- 7.1 The Supplier shall collect audit Records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit Records should (as a minimum) include regular reports and alerts setting out details of access by End Users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.
- 7.2 The Parties shall work together to establish any additional audit and monitoring requirements for the Information Management System.
- 7.3 The retention periods for audit Records and event logs must be agreed with the Authority and documented in the Security Management Plan.

8 LOCATION OF AUTHORITY DATA

The Supplier shall not and shall procure that none of its Sub-contractors Process Authority Data outside the United Kingdom unless all of the requirements of sub-Clause 24.6(c) (*Protection of Personal Data*) are met.

9 VULNERABILITIES AND CORRECTIVE ACTION

- 9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated through a Vulnerability Correction Plan will present an unacceptable risk to the integrity of the Authority Data.
- 9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'High', 'Medium' or 'Low' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:
- (a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'Critical', 'High', 'Medium', 'Low' and 'None' respectively (these in turn are aligned to CVSS v3.0 scores as set out by NIST at <http://nvd.nist.gov/cvss.cfm>);
 - (b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively; and
 - (c) Any other vendors' security advisory categorisation service as used in the Supplier Information Management System
- 9.3 Subject to Paragraph 9.4 of this Annex A1, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System in accordance with NCSC vulnerability Management guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/vulnerability-management>. Depending on severity of the vulnerabilities assessed by the supplier, patches should be deployed within:
- (a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical'; and
 - (b) thirty (30) days after the public release of patches for all non-Critical categories or patches.
- 9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 9.3 of this Annex A1 shall be extended where the:
- (a) application of a security patch adversely affects the Supplier's ability to deliver the Goods and/or Services. In which case the Supplier shall be granted an extension to such timescales of five (5) days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority and alternative mitigating controls, agreed with the Authority, are put in place and monitored until the patch has been applied; or
 - (b) Authority agrees a different maximum period after a case-by- case consultation with the Supplier under the processes defined in the Security Management Plan.
- 9.5 The Security Management Plan shall include provisions for major version Upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing. All COTS Software must be no more than N-1 versions behind the latest New Release.
- 9.6 If the Supplier fails to patch vulnerabilities in the Information Management System in accordance with Paragraphs 9.3 to 9.5 of this Annex A1, such failure shall constitute a material Default by the Supplier and the Authority may by terminate this Agreement with immediate effect as an Emergency Exit by issuing a Termination Notice to the Supplier.

10 SECURE ARCHITECTURE

- 10.1 The Supplier shall design the Information Management System in accordance with:

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

- (a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/collection/cyber-security-design-principles>;
- (b) the NCSC "Bulk Data Principles", a copy of which can be found at <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data> ; and
- (c) the NCSC "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles> and which are summarised below:
 - (i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
 - (ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
 - (iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
 - (iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Goods and/or Services and information within it;
 - (v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Goods and/or Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
 - (vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
 - (vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Goods and/or Services be designed and developed to identify and mitigate threats to their security;
 - (viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;
 - (ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
 - (x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
 - (xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Goods and/or Services should be identified and appropriately defended;
 - (xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
 - (xiii) "Cloud Security Principle 13: audit information for users" which, amongst other

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

matters, requires the Supplier to be able to provide the Authority with the audit Records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and

- (xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

10.2 The Supplier shall design the Information Management System to ensure Availability commensurate with the Target Performance Levels (as defined in Schedule 2.2 (*Performance Levels*)). This will also include consideration of the:

- (a) resilience of the Service components;
- (b) resilience and recovery of the Authority Data stored in the Information Management System; and
- (c) the Service Continuity Plan.