Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE: **TfL 96078**

THE BUYER: **Transport for London**

BUYER ADDRESS 5 Endeavour Square, LONDON, E20 1JN

THE SUPPLIER: Edenred (UK Group) Ltd

SUPPLIER ADDRESS: 50 Vauxhall Bridge Road, London, SW1V 2RS

REGISTRATION NUMBER: 00540144

DUNS NUMBER: 210186342

SID4GOV ID: N/A

CUSTOMER HR/COMMERCIAL CONTACT

Name: [redacted]	Position: Senior Category Manager
Telephone: N/A	E-mail Address: [redacted]
Postal Address: 14 Pier Walk London SE10 0ES	
Town/City: London	Post Code: SE10 0ES

CUSTOMER ORDER CONTACT

Name: [redacted]	Position: Head of Reward and Recognition
Name: [redacted]	Position: Reward and Recognition Specialist
Telephone: [redacted]	
E-mail Address: [redacted]	
Postal Address: Floor 4, 200 Buckingham Place Road,	
Town/City: London	Post Code: SW1W 9TJ

CUSTOMER INVOICING CONTACT

Telephone: 0343 222 5100	E-mail Address: invoices@tfl.gov.uk
Postal Address: Accounts Payable, P.O. Box 45276, 14 Pier Walk, SE10 1AJ	
Town/City: London	Post Code: SE10 1AJ

CUSTOMER DATA PROCESSING SECURITY OFFICER

Name: Richard Bevins, Data Protection Officer, DPO@tfl.gov.uk,
Department: For cyber incident contact [redacted]

CUSTOMER DELIVERY ADDRESS FOR ANY GOODS
TfL has multiple offices, depots and other locations. As such as delivery of goods would be confirmed at the relevant time for the relevant delivery location

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 01.03.2023 of issue.
It's issued under the Framework Contract with the reference number **RM6133** for the provision of Employee Benefits.

CALL-OFF LOT(S): N/A

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing, we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

2. *Joint Schedule 1(Definitions) RM6133*
3. *The following Schedules in equal order of precedence:*
   - *Joint Schedules for RM6133*
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)
     - Joint Schedule 4 (Commercially Sensitive Information) – **Call Off Schedule 5 pricing information**
     - Joint Schedule 6 (Key Subcontractors) **Defined in Call off Deliverables**
     - Joint Schedule 7 (Financial Difficulties)
     - Joint Schedule 8 (Guarantee)
     - Joint Schedule 9 (Minimum Standards of Reliability)
     - Joint Schedule 10 (Rectification Plan)
     - Joint Schedule 11 (Processing Data) **Defined in Call -Off Schedule 20 (Call-Off Specification) SERVICE DESCRIPTION – Section K**
     - Joint Schedule 12 (Supply Chain Visibility)
   - *Call-Off Schedules for **RM6133***
     - Call-Off Schedule 1 (Transparency Reports)
     - Call-Off Schedule 2 (Staff Transfer) – **NOT USED**
     - Call-Off Schedule 3 (Continuous Improvement)
     - Call-Off Schedule 5 (Pricing Details) - **See Below**
     - Call-Off Schedule 6 (ICT Services) – **See Below**
     - Call-Off Schedule 7 (Key Supplier Staff) **– See Below**
     - Call-Off Schedule 8 (Business Continuity and Disaster Recovery) – **See Below**
     - Call-Off Schedule 9 (Security) – **See Below and complete schedule at the end of this Framework Schedule**

- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 11 (Transparency Reports)
- Call-Off Schedule 12 (Clustering)
- Call-Off Schedule 13 (Implementation Plan and Testing)
- Call-Off Schedule 14 (Service Plans)
- Call-Off Schedule 15 (Call- Off Contract Management)
- Call-Off Schedule 16 (Benchmarking)
- Call-Off Schedule 17 (MOD Terms) – **NOT USED**
- Call-Off Schedule 18 (Background Checks)
- Call-Off Schedule 19 (Scottish Law – **NOT USED**)
- Call -Off Schedule 20 (Call-Off Specification) – **See Below Service Specification**
- Call-Off Schedule 21 (Northern Ireland Law) – **NOT USED**

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility) RM6133
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS
The following Special Terms are incorporated into this Call-Off Contract:

1. Should the Deliverables under the Call-Off Contract include any of the following Services:
   a) Financial Wellbeing;
   b) Green Cars;
   c) Payroll Giving; or
   d) Cycle to work,
   as these Services constitute regulated financial activities or have other regulatory requirements, the Buyer will be required to sign an agreement directly with the Supplier's Subcontractor, being the provider of those Services, in addition to the Call-Off Contract, in a form to be agreed between the Buyer and the Subcontractor.

2. TfL has the right to terminate their Call-Off Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice.

CALL-OFF START DATE: 01/04/2023

CALL-OFF EXPIRY DATE: 31/03/2026 with the option to extend for one further year.

CALL-OFF DELIVERABLES

Online Employee Benefits Platform. The Supplier shall provide an Online Employee Benefits Platform together with maintenance of the said platform to the Buyer(s) to deliver the following benefits:

	Service	**Description**	**Sub- con-tractor**	**YES/NO**

CORE				
Car	**Green Car Scheme**	The Supplier shall provide a Green Car Scheme that provides access to the Public Sector Discounts available from car manufacturers, and include car insurance, servicing, maintenance, repair, and breakdown cover.	Tusker	**NO**
CCV	**Childcare Voucher Scheme**	The Supplier shall provide childcare vouchers covering all types of childcare provision.	Edenred	**YES**
C2W	**Cycle to Work Scheme**	The Supplier shall provide an HMRC approved Cycle-to-Work Scheme that includes the provision of cycles and cycle safety equipment supplied through approved cycle outlets nationwide. The scheme shall adhere to the Department of Transport Cycle to Work policy.	Cycle Solutions	**YES**
ED	**Employee Discounts Scheme**	The Supplier shall provide employee discounts on a range of goods and services. These shall appeal to the diverse employee base of the Buyers and shall include branded high street names as well as local offers.	Edenred	**NO**
Gym 1	**My Gym Discounts**	The Supplier shall provide a discounted gym memberships to cover gyms and leisure centres as well as exercise and fitness classes delivered through high street names, independent and local providers.	Incorpore	**NO**
Gym 2	**Gym Flex**	As above but, payroll deducted.	Incorpore	**NO**
Payroll	**Payroll Giving Scheme**	The Supplier shall provide an HMRC approved Payroll Giving Scheme to allow employees to give money to UK registered charities of their choice from their gross pay.	Charities Trust	**NO**
R&R	**Reward and Recognition Scheme – Compliments Select & Connect Recognition**	Compliments Select and Connect Recognition Portals to be used for the provision of Long Service, Make a Difference and ad hoc vouchers, as well as offline fulfilment.	Edenred	**YES**
Tech	**Technology Smartphone Discount Scheme**	The Supplier shall provide technology and smartphone discounts to employees including discounts on the latest technology from leading manufacturers.	Let's Connect	**NO**

Well Being	**Financial Wellbeing Scheme**	The Supplier shall provide an online financial education service and a range of products and services aimed at improving employees' financial well-being.	Salary Finance/ Cushon	**NO**
ADDITIONAL				
Dental	**Dental Insurance**	The benefit gives employees access to a dental insurance policy, at corporate rates, to help make costly and essential dental treatment more affordable. The policy allows the employee to claim towards insured dental treatment from day one They are covered for pre-existing conditions,excluding mouth cancer, and they are covered for planned or pending treatment with their choice of NHS or private dentist. There are three levels of cover and partners or children can also be included.	UNUM	**NO**
Health 1	**HealthiFlex (Health Screening)**	Corporate discounts on health assessments, delivered through a network of suppliers located nationally.Additional services to complement the scheme include but are not limited to digital GP services, virtual physio, nutrition and lifestyle coaching, and counselling.	Incorpore	**NO**
Health 2	**MyHealth Discounts**	As above, but non-payroll.	Incorpore	**NO**
Additional				

Description	**Dates**
Annual Fee	
Recognition (Compliments Connect)	01April 23 - 31 March 24 01April 24 - 31 March 25 01 April 25 - 31 March 26 01 April 26 - 31 March 27 (Optional 12-month Extension)
Other:	
Long Service Vouchers	Monthly on actuals (divide total by12)
Long Service Printing and Frames	Monthly on actuals (divide total by12)

CCV Admin Fee	Monthly [redacted] on actuals

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £[redacted] MAXIMUM Estimated Charges in the first 12 months of the Contract.

PAYMENT METHOD
BACS

BUYER'S INVOICE ADDRESS:
Accounts Payable, P.O. Box 45276, 14 Pier Walk, SE10 1AJ

BUYER'S AUTHORISED REPRESENTATIVE
[redacted] (as above)

BUYER'S ENVIRONMENTAL POLICY
Non-Stated

BUYER'S SECURITY POLICY
TfL Cyber Security Management Schedule (Call of Schedule 9 with the complete schedule at the of this Framework Schedule 6.

Call-Off Schedule 7 (Key Supplier Staff)
SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted] Account Manager
50 Vauxhall Bridge Road London, SW1V 2RS

SUPPLIER'S CONTRACT MANAGER
[redacted] Contracts Manager
[redacted]

Review MEETING FREQUENCY
A minimum of Quarterly, but as required monthly

KEY STAFF
Senior Project Manager[redacted]
Senior Data Security Officer: [redacted]

KEY SUBCONTRACTOR(S)
As above

COMMERCIALLY SENSITIVE INFORMATION
Pricing

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
Not applicable

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Role:	[redacted]	Role:	[redacted]
Date:	[redacted]	Date:	[redacted]

1.Call-Off Schedule 5 (Pricing Details)

Description Annual Fee	Dates	Cost per annum per Employee (excluding VAT)	Totals
Recognition (Compliments Connect)	01 April 23 - 31March 24 01 April 24 - 31March 25 01 April 25 - 31March 26 01 April 26 - 31 March 27 (Optional 12-month Extension)	[redacted]	Tbc based on actual headcount

	Recognition fulfilment Product / Service	Unit	Unit Charge
	Long Service Award Packs		
L1	Personalised, (name & year, Chief Officer name & job title) and proof checked certificate, on A4 quality paper with foiling (as per sample)	Each	[redacted]
L2	A4 Frame (as per sample) Boxed, A4 Silver, cushioned, pull out back	Each	[redacted]
L3	Packaging and Courier of batch of award packs to TfL (Same day courier - packs covered against any loss up until being delivered andsigned for by TfL)	Each	[redacted]
L4	Packaging and First-Class postage of individual award pack,	Each	[redacted]
	Make a Difference Team Award Packs		
A1	Personalised, (Team name, citation, date) and proof checked certificate:Team on A4 paper with foiling	Each	[redacted]
A2	Letter for inclusion re Team Award	Each	[redacted]
A2	A4 Perspex frame with feet	Each	[redacted]
A4	Packaging and First-Class postage of award pack, (team or in-dividual)including frame, lapel pin/s on backing card - provided by TfL, (or if provided by supplier to a design agreed), to award recipients LineManager	Each	[redacted]
	Postage of gift cards		
	The postage cost for gift cards, selected by employees from the catalogue (NB the majority of the redeemed catalogue items are likely to be eCards where there is no handling / postages costs)	Each	[redacted]

The Supplier will manage the stock of materials and, when further quantities are required, will provide a quote for TfL approval. If the cost of supplying the products or services above, increases then the Supplier reserves the right to request an increase in its Unit Charge.

Call -Off Schedule 20 (Call-Off Specification) SERVICE DESCRIPTION

A. Cycle to Work – Salary Sacrifice Voluntary Benefit

B. Childcare Vouchers – Salary Sacrifice Voluntary Benefit

C. Recognition

   1. Long Service Awards
   2. Team Make a Difference Awards
   3. Make a Difference Platform (Connect)

D. Account Management

E. Technical Requirements

F. Accessibility & Quality Standards

G. Cyber Security

H. Disaster Recovery and Business Continuity

I. Data Transfer

J. Critical Service Failure

K. Processing, Personal Data and Data Subjects

1. SERVICE REQUIREMENTS

A. Cycle to Work (C2W) - the following requirements are essential:

1. The Cycle provision must provide a wide range of bicycles that caterer for novice to experienced bike riders, as well as electric bicycle options and safety accessories. The provision must be withing a cost limit set by TfL.
2. The Cycle to work salary sacrifice scheme must be Government compliant and allow options of both anytime enrolment and twice annual election windows
3. There must be a secure online 24/7 access, via the TfL reward hub, using single sign, giving employees access to elect the cycle to work benefit on-line
4. There must be employee access to instant online hire agreements and online acceptance of agreement
5. Hire agreement options to include
   a) A 12 month hire agreement (essential)
   b) An additional 18 month hire agreement (desirable)
6. At the end of the hire agreement there must be options for:

   Option 1 – Extended Use Agreement - enabling employees to continue the terms of the original Agreement through an extended usage arrangement directly with the Cycle to Work provider.

   Option 2 – Immediate Purchase of the equipment - enabling employees to take ownership of the equipment.

   Option 3 – Return of the equipment - collection of unwanted bicycles/equipment directly from the employee.
7. Employee must be able to view their election and corresponding payroll deductions at any point in time via the Reward Hub using single sign on.

8. Must be able to provide reports that enable the feed of the Cycle to Work records to SAP HRS and SAP payrolls including election records (as referred to in E.13).
9. Transfer of data must be enabled through secure file transfer e.g., GoAnywhere
10. Must facilitate an approval process during the enrolment process, to ensure the National Minimum Wage is not breached.
11. Must accommodate benefit elections by those under 18 years of age using an agreed offline process.

B. Childcare Vouchers (CCV) - the following requirements are essential

1. The childcare voucher salary sacrifice scheme must be Government compliant and the CCV vouchers must be accepted by a wide range of registered (ag by Ofsted) childcare providers.
2. There must be a secure online 24/7 childcare voucher account management solution, via the Reward hub platform using single sign on where employees can directly manage their childcare payments with their registered providers. This must include change of contributions or ceasing membership
3. Must be able to issue refunds of CCVs in exceptional circumstances subject to TfL approval
4. Must be able to provide reports that must be optimised for automatic feed of the Childcare Vouchers records to SAP HRS and SAP payrolls (as referred to in E.13)
5. Transfer of data must be enabled through secure file transfer, e.g., GoAnywhere
6. If the Government changes the current decision and communicates that CCV schemes should be reopened to new applicants, this change must be accommodated to allow the maximum number of employees the opportunity to join the CCV scheme
7. Instant online agreements and online employee acceptance of agreement must be provided
8. Must be able to accept transfer of any TUPE CCV arrangements as and when required

C: Recognition TfL

1. <u>Recognition TfL - Long Service</u>

1.1 Long Service in TfL is formally celebrated at 25 and 40 years. Individuals receive a financial gift, which for 25 years is currently [redacted] and for 40 years is currently [redacted]. They also receive a framed signed certificate, and lapel pin.

1.2 Occasionally TfL has the requirement to place urgent orders outside of the standard process, outlined below. The Service Provider needs to work flexibly with such requirements. Single, ad hoc orders for Long Service Awards may be sent via First Class post if agreed with TfL's Long Service Awards contact.

<u>1a: Long Service Framework</u>

Award	Award Pack and contents	Criteria	Approved by
Long Service 25 years award	• [redacted] Voucher • A4 personalised 25-year certificate (LUor TfL) • Boxed, A4 Silver, cushioned, pull outback	Employees who have completed either25 years continuous or aggregated service	Must be in service at anniversary date
Long Service 40 years award	• [redacted] Voucher • A4 personalised certificate (LU or TfL)	Employees who have completed either40 years con-	Must be in service at anniversary date

	• Boxed, A4 Silver, cushioned, pull outback	tinuous or aggregated service	
Adhoc Long Service award	• A4 personalised certificate • Boxed, A4 Silver, cushioned, pull outback	Special request normally by Exec /Commissioner's office	Pensions & Reward Director

1b: Stock

1. Edenred will hold a base certificate stock for overprinting and A4 Silver Frames. Edenred and TfL will agree minimum stock levels for each item. Edenred will inform TfL when stock is approaching threshold. This will in good time to prevent any interruption of service, and TfL will confirm the required quantity to be reordered. Edenred will provide TfL with a quote covering item, quantity and unit price, for TfL approval.
2. The Edenred Compliments Select site will be accessed by TfL to provide vouchers for eligible employees.
    a) Edenred will provide a branded voucher template for 25- and 40-years vouchers.
    b) Edenred will provide a branded redemption site for employees to redeem vouchers.
    c) TfL Long Service Awards team to place the order online monthly / as required.
    d) Each employee will receive the full details of the voucher to their work email address including how to redeem it and the expiry date. On certain occasions vouchers will be emailed to personal email address.
    e) Edenred will provide access to a helpdesk for resolution of voucher fulfilment issues – (currently helpdesk-uk-vbr@edenred.com 01244 625400 / 0333 400 1185)
3. Edenred under instruction from TfL need to have the ability to remove catalogue items that are not in keeping with TfL standards

1c: Data

1. TfL to email Long Service data, in password protected files, to a designated email address at Edenred, every four weeks / at agreed times (Circa 20 to 100 in each order). On certain occasions ad-hoc requests for one award may also be submitted. The data will include the following:

Employee No	Title	First Name	Last Name	Certificate Signatory Name (e.g., CO)
Milestone (25 or 40 years)	Date Entered Service	Mode	Business Area	

1d: Process

1. Edenred will overprint required details on correct certificate and quality check.
2. Edenred will place each certificate in a labelled 'do not bend' envelope.
3. Edenred will securely pack the order of certificates and frames and courier to TfL:
    a) PA to Director of Pensions and Reward, Floor 4, 200 Buckingham Palace Road, London SW1W 9TJ. (Change in delivery and contact details will be advised as appropriate).
4. The SLA from receipt of data to dispatch will be as follows:

Fulfilment	KPI	Target KPI	Red (Unac-ceptable)	Amber (Improve-ment needed)	Green (Acceptable)
Long Service batch process	96 hours, (4 working days)	100%	<90%	>=90%-95%	>=95%
Urgent Individual Long Service	48 hours (2 working days)	100%	<90%	>=90%-95%	>=95%

1e: Compliments Select Online Vouchers (also refer to 1a)

1. Edenred will record the Serial Number of the voucher against employee name after each order made byTfL for reference.

1f: Management Information

1. Edenred to provide MI for any order placed by TfL upon request.

1g: Invoices

1. Edenred will provide the following invoices, to a format agreed with TfL every four weeks / following each order: -
   a) Long Service Award Vouchers to be emailed to TfL Long Service contact quoting correct LongService Award PO number.
   b) Long Service Award Collateral to be emailed to TfL Long Service contact quoting Long Service Award PO number.
   c) The final and agreed invoices above to be emailed to rrtflinvoices@tfl.gov.uk. TfL Long Service contact will confirm and good receipt the invoice in SAP and forward on to Accounts Payable to process the payment.

1h: Liabilities

1. Any loss incurred as a result of instances where codes are reported as redeemed by someone other than the intended employee will be the liability of TfL. Edenred will work with TfL to share redemption information as far as is permitted by relevant legislation and Edenred's own Data Protection Policy.

1i: Cessation of Fulfilment

1. TfL can order at any time for the fulfilment of any TfL Long Service item outlined in A1 to cease. At this time the following will occur:
2. Any outstanding stock will be returned to TfL, subject to orders being agreed with TfL, as per 1b. Costs applied will be in line with the pricing schedule.

2. Recognition TfL - Make Difference Team Award Fulfilment

1. Make a Difference is TfL's recognition scheme which includes the offline fulfilment of Make a Difference TeamAwards.

2a: Make a Difference Framework

Team Awards	• One A4 foiled certificate for the team • Frame (with detachable feet forstanding / hanging on wall) • Covering letter with info and contactdetails	Teams that have gone above and beyondand made a real impact on our ability to deliver our priorities, whilst role modellingour Values. Teams are made up of employees andNPLs. A team is where three or more people arebeing recognised for working on the same activity.	Band 4 or above

2b: Stock

1. Edenred will hold a base certificate stock for overprinting and A4 Perspex frames with feet. Edenred and TfL will agree minimum stock levels for each item. Edenred will inform TfL when stock is approaching threshold, in good time to prevent any interruption of service, and TfL will confirm the required quantity to be reordered. Edenred will provide TfL with a quote covering item, quantity and unit price, for TfL approval.

2c: Data

1. TfL will email Team Make a Difference data, in password protected files, to a designated email address at Edenred, twice weekly. (Normally Monday, or next working day if Bank Holiday).
2. The data will include the following: -

Team Make a Difference Award	Team Name	Date of award (month / year)	Citation (300 characters)	Name and Address for Posting

2d: Process

1. Edenred will overprint required details on the Team certificate and quality check.

2. Edenred will print letters, package certificates with reward collateral into an Award Pack to include:
    a. Team – covering letter, One Team certificate and frame

3. Edenred will send each pack to the designated recipient via first class post, (or if a number ofrecipients at the same address by courier at Edenred's discretion).
    a. The SLA from receipt of data to dispatch will be as follows

Fulfilment	KPI	Target KPI	Red (Unacceptable)	Amber (Improvement needed)	Green (Acceptable)
Make A Difference Team Certificates	48 hours, (2 working days)	100%	<90%	>=90%-95%	>=95%

2e: Management Information

1. Edenred will provide MI for Make a Difference to TfL every month, to a format agreed with TfL in support of each invoice, including the allocation of Make a Difference Collateral

2f: Invoices

1. Edenred will provide the following invoices on a monthly basis: -
    a) Make a Difference Collateral copy to be emailed to be emailed to TfL Make a Difference contact quoting correct Make a Difference PO number

Invoices					
Issue of Make a Difference Invoice, MI and SLA data	By the 8th of every month	100%	<90 %	>=90%-95%	>=95 %

2g: Liabilities

1. Any loss incurred as a result of instances where codes are reported as redeemed by someone other than the intended employee will be the liability of TfL. Edenred will work with TfL to share redemption information as far as is permitted by relevant legislation and Edenred's own Data Protection Policy.

2h: Cessation of Fulfilment

1. TfL can order at any time for the fulfilment of any Make a Difference item outlined in 2a to cease. At this time the following will occur:
    a) Any outstanding stock will be returned to TfL, subject to orders being agreed with TfL, as per 2a. Costs applied will be in line with the pricing schedule.

3. Recognition – Make a Difference Platform - The following requirements are essential

a. Must be able to provide an online recognition platform, with the requirements listed below for all TfL employees, (c27,000)

b. Must be able to provide an 'end to end' recognition process via an accessible recognition platform

c. Must be able to escalate recognition through the TfL hierarchical structure for consideration for either an individual or a team recognition award

d. Must have ability for TfL 'self-service' the recognition platform for 'day to day' requirements, including screen updates and communications

e. Must have ability for secure file transfer of SAP data, with the addition of hierarchical and date entered service

f. Must have easily accessible real time 'dashboards' of recognition activity at all levels from line manager's team to organisational

g. Must be able to highlight TfL key behaviours/values/ priorities, making them highly visible and an integral part of the recognition nomination, approval and award process

h. Must be able to produce, to a design approved by TfL, an 'editable' 'certificate' that can electronically kept either for printing locally or centrally, (internally or externally by supplier) for presentation to employee / team

i. Must be able to allocate a financial catalogue 'gift' to individuals, with the individual being automatically notified and their catalogue account being automatically credited
    a. Must have agreed process with TfL for leavers with catalogue balance
    b. Edenred under instruction from TfL need to the ability to remove catalogue items that are not in

keeping with TfL standards.

c. Must have the ability to work with TfL on any transfer of catalogue funds to a new provider, if required at the end of the contract.

d. Unspent funds on employee's catalogue accounts remain the property of TfL and must be returned toTfL on request, at no extra cost to TfL.

j. Must be able to manage budgets centrally as well as locally.

k. Must be able to extract raw data of all elements of the award, including reason and behaviour and convert it to Excel, running reports, to include weekly SAP uploads.

l. Must have ability for nominations for special awards to be made and reviewed through the recognition platform, separate to the main nomination process

m. Special Occasion Digital E cards **-** Must have the ability for a selection of ecards, (agreed with TfL) to be available for employees to send to each other as a thank you and on special occasions including birthdays, anniversaries etc.

n. Must continue to develop and configure the platform and process with consideration of TfL's requirements and developments in recognition.

The following requirements are desirable:

o. Ability for an Open Application Programming Interface – To enable integration with Yammer to promote culture of recognition and engagement.

p. The ability for nominations for batches of awards to be made and reviewed through the recognition platform, separate to the main nomination process

D. **Account Management -** the following requirements are essential

1. Edenred will work with TFL to provide expert knowledge across benefits and recognition. For risk-based benefits we suggest FCA regulated advice.
2. Must proactively keep TfL abreast of developments and innovations and how these can be delivered and communicated to add value to TfL's proposition and employee engagement
3. Must have expert ability to provide specialist support to drive high Make a Difference platform adoption and engagement across all the components included in this specification and share industry good practice
4. The Technical helpdesk must be available during normal office hours Monday to Friday to record and handle queries, provide 1st Line support, and record and forward incidents
5. Must have formal contractual arrangements in place with any third-party Business Service parties for the life of the contract with TfL
6. Must have clear processes in place for handling complaints
7. Must meet jointly agreed Service Level Agreements (SLAs) SLAs to be reviewed on regular basis :

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure
Accurate and timely billing of Customer	Accuracy /Timelines	[redacted]

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure
Access to Customer support	Availability	[redacted]
Complaints Handling	Availability/Timelines	[redacted]
provision of specific Goods and/or Services	Quality	[redacted]
Timely provision of the Services As per Order Form Appendix E	Services Availability	[redacted]

E Technical Requirements - Make a Difference Platform (Connect) Cycle to Work online solution, Childcare Vouchers online solution Call-Off Schedule 6 (ICT Services)

The following requirements are essential

a. Must provide 24/7 access to an online solution. Routine maintenance will be scheduled for out of hours and TFL will be notified in advance. In the event of emergency maintenance / an outage, Edenred must notify TFL within 15 minutes by email:

   Service owners

   A) [redacted]
   B) [redacted]
   Copying in IMMajorIncidents@tfl.gov.uk

   For any major incidents, as well as the Service Owners, the T&D Major Incidents – IMMajorIncidents@tfl.gov.uk team must be kept informed to enable a major incident alert to be circulated and TSO Professional Services – SAP Team - SAPServiceDelivery@tfl.gov.uk & [redacted] must be notified of the system outage

b. Solutions must cater for detection of failures as they occur and these must be resolved within 2 hours.

c. Solutions must be able to manage spikes or surges in demand that may have the potential to negatively affect the performance

d. Solutions must support scalability of the application in a coherent and non-disruptive manner. This is both from the perspective of TfL demand and the wider usage of the application by other customers of the vendor

e. Solutions hosted outside of TfL technical Infrastructure but available to be accessible via TfL corporate devices

f. Solutions must have development, test & productions systems, for effectively managing change/updates

g. Solutions must be able to be branded, including customised web layout, imagery and tailoring the look and feel to TfL requirements,

h. The solutions must be resilient, use industry standard best practice, have high availability and be able to failover, if required

i. The Make a Difference (Connect) Platform must be a SAAS / Cloud based hosted solution and must be accessible via the desktop and/or mobile device

j. All systems and processes must fully adhere to General Data Protection Regulations (GDPR) (see K. Processing, Personal Data and Data Subjects)

k. All systems must support Single sign on using TfL's active directory login credentials without the user needing to specify their login details (if already logged in to TfL network)

l. All third-party technology services and assets must be fully and formally supported by contracts with reputable companies

m. The system must be able to support, via agreed reports, incoming Interface from SAP (ECC6,EHP5) via Batch data exchange. In the future TfL will be using Success Factors (EC)

n. TfL data in transit must be encrypted as per the Information Classification Protection Requirements (see K. Processing, Personal Data and Data Subjects, G. Cyber Security, I. Data Transfer)

o. System access must be revoked by disabling accounts either upon termination of an employee, or at an agreed future timeline i.e., two months post termination.

F. Accessibility & Quality Standards

a. Must be able to develop, host and maintain online solutions for access to services listed under 'Contract Requirements', which is compliant with TfL's required online standards in accessibility Level 'AA' of the WAI's Web Content Accessibility Guidelines (WCAG 2.1)) as a minimum standard. Guidance can be found at TfL's Digital Accessibility Standard (https://tfl.gov.uk/info-for/suppliers-and-contractors/digital-design-toolkit/digital-accessibility-standard) and Digital Accessibility https://tfl.gov.uk/corporate/website-accessibility/

b. Must comply with TfL's Corporate Design Standards (https://tfl.gov.uk/info-for/suppliers-and-contractors/design-standards)

G. Cyber Security Call- Off Schedule 9 (Full Schedule at the end of this Framework Schedule 6)

a. Must comply with TfL Cyber Security Management Schedule v1.017 (Call Off Schedule 9 and in full at the end of this Framework Schedule 6

b. Must undertake periodic penetration and security testing and alert TfL of any risks.

c. Must continue to uphold compliance to ISO 27001:2013 and Cyber Essentials Plus Scheme.

H. Disaster Recovery and Business Continuity (Call – Off Schedule 8)

a. Must have formal documented recovery plans to identify the resources and specify actions required to help minimise losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable. Edenred Business Continuity Disaster Recovery Plan Doc 8.3.1.pdf

I. Data Transfer

a. Must be secure and encrypted. Current secure file data transfer via GoAnywhere

J. Critical Service Failure

a. In relation to all the online solutions including the Connect Platform, known in TfL as the Make a Difference Platform, a Critical Service Failure shall mean a loss of two (2) or more hours during core hours (08:00 – 18:00 Mon – Fri excluding bank holidays) for more than 24 hours accumulated in three (3) Month period, or 48 hours in any rolling twelve (12) month period. –

b. The default period is three months if less than three months is required then an alternative period should be inserted above.

K. Processing, Personal Data and Data Subjects Joint Schedule 11 (Processing Data)

PART A - PROCESSING, PERSONAL DATA AND DATA SUBJECTS

Introduction

a. The contact details of Edenred's Data Protection Officer are: [redacted] Data Protection and Compliance Officer, [redacted]

b. The contact details of the Transport for London's Data Protection Officer are: [redacted] | [redacted]

c. The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated as below

Description	**Details**
Identity of the Controller and Processor	TfL is the Controller and Edenred is the Processor for the personal data that TFL, transfers to Edenred for the purposes of providing licences and the services described in Call -Off Schedule 20 (Call-Off Specification) SERVICE DESCRIPTION. Edenred and TfL are Joint Controllers for: the processing of employee data necessary for the communication and delivery of services to TfL employees who have signed up to the services provided through described in this Framework Schedule 6 Call Off Contract. Where Edenred is a processor, it will process Personal Data from TfL in accordance with written instructions from the TfL to perform its obligations under the Contract.
Subject matter of the processing	The processing is needed to ensure that an effective and timely employee benefits and recognition products and services are provided to employees.
Duration of the processing	1/04/2023 – 31/03-2026 (option to 31/03/2027)

Nature and purposes of the processing	The nature of the processing means any operation such as 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 of data (whether or not by automated means) etc. The purpose of the processing is to provide employee benefits and recognition products and services to employees.
Data breach	Edenred will notify TfL without undue delay and in any event within 72 hours by written notice with all relevant details reasonably available of any actual or suspected data breach.
Type of Personal Data	The personal data processed by Edenred as Data Processor to TfL consists of Employee data, such as employee number, names, date of birth, email address, postal address, to validate the data subject is a permanent or fixed term contract employee of Transport for London. In addition to the data subject's grade and business area for the purposes of Management Information. The personal data processed by TfL and Edenred as Joint Controllers relates to employees who have signed up to the services provided through the employees benefits and recognition products. This data includes log in data such as IP address, records of website visits and transactions. address details, proof of identity and employee contact details.
Categories of Data Subject	Staff (permanent staff and fixed term contract)
Plan for return and destruction of the data once the processing is complete **unless** requirement under union or member state law to preserve that type of data.	● Edenred retains customer data for the duration of the contract. ● Upon termination Edenred will remove your data within 90 days. ● Customer's order history may be retained by Edenred for Six years from the date of customers order in case of a dispute. ● Edenred Privacy Notice (https://www.edenred.co.uk/en/privacy-policy/)

PART B – JOINT CONTROLLER AGREEMENT The essence of this relationship shall be published. The Parties may wish to incorporate some clauses equivalent to those specified in clause.

The Parties may also wish to include an additional clause apportioning liability between the parties arising out of data protection of data that is jointly controlled.

Where there is a Joint Control relationship, but no controller to processor relationship under the contract, this completed Part B should be used instead of

The following Part B applies to Personal Data under the Joint Control of the Parties as described in clause K (Service Requirements of this Contract.

1. The Service Provider shall be responsible for the provision of information to Data Subjects as detailed in GDPR Article 13 (Information to be provided where personal data are collected from the data subject).
2. The Customer shall be responsible for the provision of information to Data Subjects as detailed in GDPR Article 14 (Information to be provided where personal data have not been obtained from the data subject).
3. The Service Provider shall be responsible for responding to any request for information from a Data Subject under GDPR Article 15 (Right of access by the data subject).
4. The Service Provider shall be responsible for responding to and rectifying any request for rectification from a Data Subject under GDPR Article 16 (Right to rectification).
5. The Service Provider shall be responsible for responding to and erasing any request for the right to erasure from a Data Subject under GDPR Article 17 (Right to erasure (right to be forgotten)).
6. The Service Provider shall be responsible for responding to and restricting any request for restriction of processing from a Data Subject under GDPR Article 18 (Right to restriction of processing).
7. The Service Provider shall be responsible for notifying any rectification or erasure of personal data or restriction of processing carried out in accordance with GDPR Articles 16, 17 and 18 to each recipient to whom the personal data have been disclosed in accordance with GDPR Article 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing).
8. The Service Provider shall be responsible for responding to and porting any request for data portability from a Data Subject under GDPR Article 20 (Right to data portability).
9. The Service Provider shall be responsible for responding to and complying with any objection from a Data Subject under GDPR Article 21 (Right to object).
10. The Service Provider shall be responsible for ensuring a Data Subject is not subject to a decision based solely on automated processing, including profiling which causes legal effects or significant effects on the Data Subject and shall comply with GDPR Article 22 (Automated individual decision-making, including profiling).
11. The Parties shall be responsible for notifying the supervisory authority (Information Commissioners Office) and the Data Subject of any Personal Data Breach in accordance with GDPR Article 33 (Notification of a personal data breach to the supervisory authority) and Article 34 (Communication of a personal data breach to the data subject).
12. Each Party shall maintain a record of its processing activities under its responsibility in accordance with GDPR Article 30 (Records of processing activities).
13. The Parties shall be responsible for carrying out a data protection impact assessment in accordance with GDPR Article 35 (Data protection impact assessment) and Article 36 (Prior consultation).

14.	The Parties agree that the Service Provider shall be the point of contact for Data Subjects.

CYBER SECURITY CALL- OFF SCHEDULE 9

TABLE OF CONTENTS

1. DEFINITIONS

"Cloud"	A type of internet-based computing service where organisation can have aspects of their IT infrastructure managed by external providers, normally as a Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) basis
"Cyber Essentials Scheme"	is a UK government scheme encouraging organisations to adopt good practice in information security, focussing mainly on technical controls rather than governance, risk, and policy
"Cyber Security Policy / Policies"	The high-level Cyber Security requirements for all IT and Operational technology and data owned by TfL or operated and supported by third parties for on behalf of TfL.
"Cyber Security Standard(s)"	The technical detail behind the implementation of the high-level cyber security requirements as set out in the Cyber Security Policies.
"Data"	means data created, generated or collected, during the performance of the Services (or any part thereof), including Personal Data and data supplied to TfL and members of the TfL Group in connection with the Services or this Agreement;
"Good Industry Practice"	means the exercise of that degree of skill, diligence, prudence, and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking under the same or similar circumstances.
HMG Information Security Assurance Standards	the meaning and definition as well as relevant policy documents and standards can be found at https://www.gov.uk/government/collections/government-security or any updated link;
"Information Asset Register"	means a register of all information assets relating to the services connected to this Agreement as detailed in paragraph 3.2(c)
"Information Security Management System" or "ISMS"	a framework of governance models, policies and procedures, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security in accordance with the requirements of Paragraph 15
ISO/IEC 27001	is an information security standard specification for an information security management system (ISMS), with an emphasis on measuring and evaluating how well an organisation's ISMS is performing.
"IT Services"	means the IT services that support the delivery of the Services;
"Malicious Software"	means any software that brings harm to a computer system. Commonly known as malware can be in the form of worms, viruses, trojans, spyware, and adware which steal protected data, delete documents or add software not approved by a user.

"Operational Technology"	means any hardware or software which monitors and/or operates a physical process.
"Outline Security Management Plan"	means the security plan provided by the Service Provider as part of their tender submission
"Removable Media"	any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives
"Security Incident"	a potential or actual event or attempted breach of security affecting the confidentiality, integrity or availability of the Services, IT Services or Networks which process or hold Data
"Security Management Plan"	means the Service Provider's security plan developed and revised pursuant to Paragraph 14
"Security Policy"	means any TfL security policies as amended by TfL from time to time;
"Security Risk"	meaning all Risks associated with the security of the Services which may have a negative impact upon the agreed security posture, including information security and any risks identified pursuant to the Security Management Schedule.
"Security Risk Register"	means a register of Security Risks produced and maintained as detailed in paragraph 3.2(b)
"Service Assets"	means all assets and rights including all physical assets, Software, IPR, as well as spares and components whether in storage, repair or on sites, used by the Service Provider to provide the Services in accordance with this Agreement;
"Service Provider Personnel"	means all employees, agents, consultants and contractors of the Service Provider or of any Sub-Contractor
"Service Provider Premises"	means any land or building where the Service Provider carries out any part of this contract
"TfL Information Security Controls Framework"	means a hierarchy of IT security documents consisting of the high-level Information Management Security Policy and ten security principles (Information Security Controls Framework);
"TfL Network(s)"	means the network infrastructure and services owned or used by TfL to support the delivery of the IT Services.
"TfL Personnel"	means all employees, agents, consultants and contractors of TfL
"TfL Restricted"	as defined in the TfL Information Security Classification Standard (listed in Annex 5)
"TfL Sites"	means all TfL premises where the services are delivered

2. SCOPE AND PURPOSE

2.1 The purpose of this Schedule is to:

(a) set out the principles of protective security to be applied by the Service Provider in its delivery of the Services;

(b) set out the Service Provider's wider security obligations relating to the Services;

(c) set out the Service Provider's requirements to test and audit the Services including any Information Security Management System, to ensure compliance with the security requirements set out in this Agreement;

(d) set out the Service Provider's obligations in the event of a Security Incident;

(e) set out the principles for the Service Provider's development, implementation, operation, maintenance and continual improvement of the Security Management Plan;

(f) set out the principles for the Service Provider's development, implementation, operation, maintenance and continual improvement of the Information Security Management System;

(g) set out any Service Provider obligation for certification against the Services such as, ISO/IEC 27001, the Cyber Essentials Scheme or HMG Information Security Assurance Standards;

(h) set out any Service Provider requirements to deliver the Services or Service Assets in accordance with the CESG Commercial Product Assurance (CPA) Scheme; and

(i) set out the requirements on the Service Provider when delivering the Service(s), which are aligned with the 10 Steps to Cyber security set out by the Government (see Annex 5).

(j) the Supplier's obligation to comply with the Operations Technology Cyber Security Standards (see Annex 5).

3. SECURITY PRINCIPLES

3.1 The Service Provider acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its provision of the Services and TfL's ability to retain public confidence. The Service Provider shall at all times comply with the security principles set out in Paragraph 3 in the delivery of the Services.

3.2 In recognition of the importance that TfL places on security, data protection and confidentiality, the Service Provider shall ensure that a director or relevant individual, as agreed by TfL, is made aware of the risks set out in the Security Management Plan and is assigned overall responsibility for ensuring that:

(a) appropriate members of Service Provider Personnel and the Service Provider's management team take responsibility for managing the different levels of security risk and promoting a risk management culture;

(b) a Security Risk Register is produced and maintained and that all Security Risks are documented in an appropriate manner and is included in any contract risk register if one is in place. This Security Risk Register must be available for audit when reasonably required by TfL as set out in Clause 7 of this Schedule

(c) an Information Asset Register is produced and maintained and that all assets are documented in an appropriate manner in the Information Asset Register and shall identify the criticality of the relevant Service Assets in the delivery of the Services. This register must be available for

audit when reasonably required by TfL as stated in Paragraph 7 of this Schedule and when a Security Incident occurs.

(d) supporting policies are implemented (where relevant) and communicated with Service Provider Personnel.

3.3 The Service Provider shall, and procure that its Sub-contractors shall, at all times ensure that:

(a) security threats to the Services are minimised and mitigated;

(b) the Services shall fully comply at all times with:

(i) any security requirements set out in Annex 3;

(ii) the agreed Outline Risk Management Processes and approach set out in Annex 2; and

(iii) Good Industry Practice.

3.4 The Service Provider must notify TfL of any instances where software, applications, services or processes are hosted or run from the cloud that are not part of the Agreement, and that host, process or connect with any of TfL Operational or IT technology, Data and Networks or handle TfL Data. The Service Provider is responsible for ensuring that any such cloud services comply with this Cyber Security Management Schedule.

4. ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS

4.1 The Service Provider shall comply with all obligations relating to the patching and configuration management of Service Assets as set out in Annex 4 in addition to any specific obligations set out in Annex 4, the Service Provider shall ensure that:

(a) security patches are applied to Service Assets as soon as possible in line with vendor recommendations in accordance with overall risk management;

(b) account management and configuration control processes are implemented to ensure that access to Service Assets by Service Provider Personnel is limited to the extent required for them to fulfil their roles in supporting the delivery of the Services.

(c) when Service Provider Personnel change roles or no longer support the delivery of the Services access rights are revoked or reviewed;

(d) any system administration functionality is strictly controlled and restricted to those Service Provider Personnel who need to have access to such functionality and that the ability of Service Provider Personnel to change the configuration of the Services is appropriately limited and fully auditable;

(e) Service Provider Personnel are informed of what constitutes acceptable access of Operational or IT technology, Data and Networks and the consequences of non-compliance;

(f) any preconfigured passwords delivered with any Service Assets are changed prior to their implementation for use in the Services;

(g) the Services have appropriate devices, tools or applications in place to filter traffic or separate connections, such as industry standard firewalls and Malicious Software protection, to all public or private networks which are not controlled by or on behalf of TfL.

(h) all wireless functionality is secure; and

(i) software upgrades and patching must be managed appropriately and access to any software shall be granted using the principle of least privilege.

5. SERVICE PROVIDER PERSONNEL

5.1 The Service Provider shall, appoint a member of Service Provider Personnel to be the security manager who shall be responsible for the development, monitoring, enforcement, maintenance and enhancement of all security measures set out in this Agreement (the "**Security Manager**"). The Security Manager shall be a member of the Key Personnel.

5.2 The Service Provider shall ensure that all Service Provider Personnel are security screened or vetted appropriate to the Data and shall provide TfL within five (5) working days of the Effective date, and every twelve (12) months thereafter, written confirmation that this obligation has been complied with.

5.3 The Service Provider shall immediately notify TfL if it becomes aware of any security clearance issues in relation to the Service Provider Personnel and the Service Provider shall undertake any action requested by TfL in relation to mitigating the impact of any such security clearance issues.

5.4 The Service Provider shall not remove or replace the Security Manager (including when carrying out Exit Management) unless:

(a) requested to do so by TfL;

(b) the Security Manager concerned resigns, retires or dies or is on maternity, paternity, adoption or long-term sick leave;

(c) the Security Manager's employment or contractual arrangement with the Service Provider or a Sub-contractor is terminated for material breach of contract by that person; or

(d) the Service Provider obtains TfL's prior written consent (such consent not to be unreasonably withheld or delayed) and the role is not left vacant.

5.5 The Service Provider shall:

(a) notify TfL promptly of the absence of the Security Manager (other than for short-term sickness or holidays of three (3) weeks or less, in which case the Service Provider shall ensure appropriate temporary cover for Security Manager);

(b) ensure that Security Manager role is not vacant for any longer than fifteen (15) Working Days;

(c) give as much notice to TfL as is reasonably practicable (and in any event twenty (20) Working Days' notice) of any intention to remove or replace Security Manager except in the cases of death, unexpected ill health or a material breach by the Security Manager of his or her employment contract;

(d) ensure that all arrangements for planned changes in the Security Manager provide adequate periods during which incoming and outgoing Security Manager work together to transfer responsibilities and ensure that such change does not have an adverse impact on the performance of the Services; and

(e) ensure that any replacement for the Security Manager

(i) is only employed or engaged with TfL's prior written consent (such consent not to be unreasonably withheld or delayed)

(ii) has a level of qualifications and experience appropriate for a Security Manager; and

(iii) is fully competent to carry out the tasks of a Security Manager whom he or she has replaced.

6. TRAINING

6.1 The Service Provider shall ensure that all Service Provider Personnel have undergone suitable security awareness training prior to their deployment and such security awareness training shall cover, as a minimum; account usage, malicious software, home and mobile working, use of removable media, audit and inspection and Security Incident reporting and data handling. The Service Provider shall implement an up-to-date on-going programme of security awareness training for Service Provider Personnel throughout the Term.

6.2 The Service Provider shall provide additional training to its Service Provider Personnel, which may be required following a Security Incident, the application of a patch or update, or any relevant Operational Change or Variation.

6.3 The Service Provider shall ensure that all Service Provider Personnel are familiar with their responsibilities under applicable law and policies including, as a minimum, the Data Protection Legislation, the Security Policies set out in Paragraph 1 of this Schedule and policies in relation to the handling of protectively marked materials both during their employment and following the termination of or change to the terms of their employment.

7. TESTING & AUDIT

7.1 The Service Provider shall conduct regular automated vulnerability scans of the Services, as agreed in the Risk Management Process and ensure that any identified vulnerabilities are appropriately mitigated or patched in line with the TfL Security Patching standard (Annex 5), taking into consideration the risk posed to TfL and the Services.

7.2 The Service Provider shall conduct security tests, including ethical hacking and penetration tests, to assure compliance with the Security Incident Management Process, the security provisions in this Agreement, the Security Management Plan. The Service Provider shall conduct security testing in accordance with the Security Management Plan. The Service Provider shall conduct such security tests, as a minimum, every twelve (12) months from the Service Commencement Date and shall include security penetration testing of the Services and the associated technical infrastructure. Wherever the Services are accessible from the internet or other such public network, the Service Provider shall carry out security penetration tests from the internet or the public network.

7.3 The Service Provider shall, within one (1) week completion of the security tests carried out in accordance with Paragraph 7.2, provide a report to TfL setting out:

(a) the outcome of such security tests including all identified vulnerabilities;

(b) the Service Provider's plans to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement [including the TfL Change Management Process and the Variation Procedure.

7.4 The Service Provider shall implement its plans to each identified vulnerability in accordance with the report delivered pursuant to Paragraph 7.3 save to the extent directed by TfL in writing.

7.5 The Service Provider shall, upon request by TfL, following a Security Incident, carry out such additional security testing over and above the obligations set out in Paragraph 7.2 as TfL requires.

7.6 TfL shall be entitled to send a member of TfL Personnel to witness the conduct of any audit or security tests carried out by or on behalf of the Service Provider. The Service Provider shall provide TfL with the results of such audits (in a form agreed with TfL in advance) as soon as practicable after the completion of each audit or test.

7.7 In addition to complying with the Requirements, PCI DSS where applicable and other relevant industry standards and Good Industry Practice, the Service Provider shall at least once during each twelve

(12) month period starting from the Service Commencement Date, engage an appropriately skilled third party to conduct a formal audit of the Services against the then current versions of the following:

(a) the security controls, processes and procedures required pursuant to this Agreement;

(b) the Data Protection Legislation (using BS10012 or another standard as agreed with TfL), where applicable; and

(c) the Security Management Plan,

and shall, within five (5) Working Days of becoming aware of actual or potential security issues which impact or could impact the Services, the Service Provider shall inform TfL of each such issue and shall keep TfL up to date as the Service Provider investigates the nature and impact of such issue. Within five (5) Working Days of the finalisation of the audit findings, the Service Provider shall provide to TfL a copy of all such findings which are relevant to the Services.

7.8 Without prejudice to any other right of audit or access granted to TfL pursuant to this Agreement or at Law, TfL and/or its representatives may carry out such audits in relation to security matters as are reasonably required to assess the Service Provider's compliance with the Information Security Management System and the Security Management Plan.

7.9 If any test or audit carried out pursuant to this Paragraph 7 reveals any non-compliance with this Agreement or vulnerability (and, in the case of a TfL audit, TfL has informed the Service Provider thereof), the Service Provider shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement including the TfL Change Management Process and the Variation Procedure. The Service Provider shall implement its plans to remedy each identified vulnerability in accordance with such report save to the extent directed by TfL in writing.

8. SECURITY INCIDENT MANAGEMENT PROCESS

8.1 The Service Provider shall, and shall procure that its Sub-contractors shall:

(a) establish, document and share with TfL a process to identify and respond to Security Incidents and mitigate the impact of such Security Incidents on the Services, including in relation to assigning clearly defined roles and responsibilities to specific Service Provider Personnel;

(b) record each Security Incident and corresponding severity level in the Service Provider's ISMS; and

(c) without limitation to the other provisions of this Agreement, follow TfL's reasonable instructions in relation to the identification and resolution of any Security Incident.

8.2 The Service Provider shall notify and ensure TfL is aware as soon as possible and, in any event, no later than within one (1) hour upon becoming aware of any Security Incident or any potential Security Incident.

8.3 In addition to the requirements in clause 8.2 the Service Provider will additionally provide written notice with all relevant details reasonably available of any actual or suspected breach of security in relation to TFL Personal Data including unauthorised or unlawful access or Processing of, or accidental loss, destruction or damage of any Authority Personal Data

8.4 If a Security Incident occurs, the Service Provider shall, within the framework of the Security Incident Management Process:

(a) immediately take steps to assess the scope of the Data, user accounts and/or TFL Personal Data compromised or affected including, but not limited to, the amount of Data and/or TfL Personal Data affected;

(b) immediately take the steps necessary to remedy or protect the integrity of the Services against any such Security Incident;

(c) securely collect and preserve evidence, including logs, to support the Security Incident management process described in this Paragraph and share with TfL such evidence via secure channels as requested by TfL;

(d) handle any information pertaining to the Security Incident according to the handling requirements for TfL RESTRICTED information defined in TfL's Information Security Classification Standard;

(e) promptly escalate the Security Incident to a person or governance forum with a level of seniority within the Service Provider's organisation as TfL may reasonably require;

(f) as requested by TfL:

(i) provide such information in relation to the Security Incident (including, if necessary, by collating such information from its and its Sub-contractors' systems and the Service Provider Personnel);

(ii) provide relevant TfL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Service Provider Sites and Service Provider Personnel in order to investigate the Security Incident; and

(iii) follow TfL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services; and

(g) as soon as reasonably practicable develop and provide TfL with a copy of its remediation plan for the Security Incident which sets out full details of the steps taken and to be taken by the Service Provider to:

(i) correct, make good, reinstate, replace and remediate all deficiencies and vulnerabilities, loss and/or damage to the Service Assets, Data, and/or Services in connection with the Security Incident; and

(ii) perform or re-perform any security tests or alternative tests relating to the security of the Service Assets and/or Services as appropriate and within the timescales specified by TfL, to assure TfL that the Security Incident has been addressed and its effects mitigated,

provided that any such remediation must be implemented in accordance with this Agreement including the TfL Change Management Process and the Variation Procedure. The Service Provider shall fully implement and comply with such remediation plan save to the extent directed by TfL in writing

8.5 The Service Provider shall provide a detailed report to TfL within two (2) Working Days of the resolution of the Security Incident, such report to detail:

(a) the nature of the Security Incident;

(b) the causes and consequences of the Security Incident;

(c) the actions undertaken and length of time taken by the Service Provider to resolve the Security Incident; and

(d) the actions undertaken by the Service Provider to prevent recurrence of the Security Incident.

8.6 If there is a suspected security event up to and including a Security Incident, the Service Provider shall to the extent requested by the TfL CISO (or any duly authorised delegate):

(a) provide information in relation to the Services which is relevant collating, if necessary, relevant information from Sub-contractors' systems and the Service Provider Personnel;

(b) provide relevant TfL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Service Provider Sites and Service Provider Personnel in order to investigate the security incident; and

(c) follow TfL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services; and

(d) work with TfL to identify any lessons learnt which could mitigate any gaps in process, policy or controls.

and TfL shall reimburse the Service Provider's reasonable, demonstrable costs and expenses in relation to the Service Provider's compliance with such request.

9. SECURITY LOGGING AND MONITORING

9.1 The Service Provider shall ensure that the Security Management Plan sets out its monitoring strategy to monitor its own performance of its obligations under this Schedule. The Service Provider shall update its monitoring strategy as necessary throughout the term of this Agreement in response to:

(a) changes to applicable laws, regulations and standards;

(b) changes to Good Industry Practice;

(c) any relevant Operational Changes or Variations and/or associated processes;

(d) any Security Incident; and

(e) any reasonable request by TfL.

9.2 The monitoring strategy should include, as a minimum, processes for monitoring and logging (as appropriate):

(a) networks and host systems to detect attacks originating both on an internal private network or from public networks (e.g., internet);

(b) instances of misuse of the Services, Service Provider systems used in the delivery of the Services and access to TfL RESTRICTED Data by TfL Personnel and Service Provider Personnel, including attempts at such misuse;

(c) wireless access points to ensure that all wireless networks are secure and no unauthorised access points are available;

(d) Malicious Software on: (i) the Service Provider systems used in the delivery of the Services and, (ii) the Services;

(e) access to and movement of TFL RESTRICTED Data, including internal access to such Data; and

(f) traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attempt or actual attack.

9.3 The Service Provider shall ensure that access to system logs and monitoring information is strictly restricted to those Service Provider Personnel who need to access these items to ensure the delivery and integrity of the Services.

9.4 The Service Provider shall ensure that any monitoring process complies with the monitoring strategy developed in accordance with Paragraphs 9.1 and 9.2 and all of its legal and regulatory obligations pursuant to Applicable Law.

9.5 The Service Provider shall maintain a log of:

(a) all instances of Service Provider Personnel accessing Personal Data;

(b) all Service Recipient, TfL Personnel and Service Provider Personnel logon attempts, successful and failed, to the Services or any elements of the Service Provider Solution requiring authentication;

(c) all actions taken by Service Recipients, TfL Personnel or Service Provider Personnel with administrative privileges;

(d) all instances of accounts being created for Service Recipients, TfL Personnel or Service Provider Personnel and their relevant privileges;

(e) all records of formal staff induction or certification required by Service Provider Personnel to operate systems and handle TFL RESTRICTED Data (where required);

(f) all instances of accounts for Service Recipients, TfL Personnel, or Service Provider Personnel being deleted;

(g) Service Provider Personnel system access group memberships in relation to relevant Service Assets;

(h) Service Recipient and group privilege changes against each of the system resources;

(i) unauthorised use of input and output devices and removable media; and

(j) all access to log files and audit systems.

9.6 The logs required in 9.5 above must be raw logs, which are provided in a structured text format and the schema for such logs will need to be provided.

9.7 The Service Provider shall implement recording mechanisms to identify TfL Personnel and Service Provider Personnel and their actions when cases of misuse are being investigated and shall ensure that any such recording mechanisms are protected against manipulation and disruption.

9.8 The Service Provider shall regularly review logs to identify: (i) anomalies; (ii) suspicious activity; and (iii) suspected Security Incidents. The Service Provider shall notify TfL of such findings in accordance with Paragraph 8.2

9.9 The Service Provider shall provide copies of any log data collected by the Service Provider during its delivery of the Services (system audit log data) at TfL's request in a human readable electronic format such as comma-separated value or Microsoft Excel.

10. MALICIOUS SOFTWARE

10.1 The Service Provider shall throughout the Term, use the latest versions of anti-malware solutions and software available from an industry accepted vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the IT Services (or as otherwise agreed by the parties).

10.2 Notwithstanding Clause 10.1, if Malicious Software is detected within services provided by the Service Provider, the Service Provider shall ensure the effect of the Malicious Software is mitigated and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Data, restore the Services to their desired operating efficiency.

10.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause 10.2 shall be borne by the Parties as follows:

(a) by the Service Provider if the Malicious Software originates from the Service Provider Software, the Third Party Software supplied by the Service Provider (except where TfL has waived the obligation set out in Clause 10.11) or TfL Data (whilst TfL Data was under the control of the Service Provider) unless the Service Provider can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by TfL when provided to the Service Provider; and

(b) otherwise by TfL.

11. REMOVABLE MEDIA

11.1 The Service Provider may only use Removable Media to support its delivery of the Services if it has obtained prior written consent of TfL and has implemented appropriate controls to ensure that the use of any input or output devices and removable media is restricted strictly to that needed to supply and support delivery of the Services.

11.2 If removable media is approved for use by TfL, the Service Provider shall ensure that it deploys suitable anti-virus and anti-malware checking solutions to actively scan for the introduction of Malware onto systems and networks through all Data imports and exports from removable media and that the removable media is encrypted to a suitable standard agreed in advance with TfL in writing.

11.3 The Service Provider shall report any loss or interception of Data as a result of the use of removable media to TfL in accordance with Clause 8 and TfL reserves the right in such instances to rescind its approval in relation to the Service Provider's continued use of removable media.

12. MOBILE AND HOME WORKING

12.1 The Service Provider may only use offer Mobile and Home working to support its delivery of the Services if it has obtained prior written consent of TfL and has implemented appropriate controls to ensure.

12.2 If such consent is granted but the Service Provider does not have a home and mobile policy for Service Provider Personnel, TfL's Home and Mobile Working Cyber Security Policy shall apply to the Service Provider and its Service Provider Personnel.

12.3 If the Service Provider has a home and mobile working policy in relation to the Service Provider Personnel, the Service Provider shall:

(a) ensure through this policy that:

(i) Data is protected and suitably encrypted in line with Cyber Security Policy (see Annex 5), when stored outside of the Service Provider Premises;

(ii) Data is protected when accessed, imported or exported through a connection other than one which is accessed at the Service Provider Premises; and

(iii) Security Incident management plans acknowledge the increased risk posed by home and mobile working such as theft or loss of Data and TfL Data and/or devices; and

12.4 The Service Provider shall report any loss or interception of Data or TfL Data as a result of home or mobile working to TfL in accordance with Clause 8.

13. DISPOSALS

13.1 The Service Provider shall not reuse any Service Asset or Removable Media used in the performance of the Services unless such items have been wiped securely in accordance with a TfL agreed standard.

13.2 The Service Provider shall securely dispose of and delete Data from Service Assets used for the delivery of the Services to a TfL agreed standard upon the termination or expiry of this Agreement or when such Service Assets are no longer required for the delivery of the Services, whichever is sooner, and documented accordingly.

13.3 The Service Provider shall ensure that the disposal of any Service Asset is accurately reflected in the Information Asset Register.

14. SECURITY MANAGEMENT PLAN

14.1 The Outline Security Management Plan as at the Effective Date is set out at Annex 1 (*Outline Security Management Plan*).

14.2 The Service Provider shall within fifteen (15) Working Days of the Effective Date submit to TfL for approval, a draft Security Management Plan which a minimum will:

(a) set out the security measures to be implemented and maintained by the Service Provider in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the Services comply with this Schedule;

(b) reference and comply with the security requirements set out in Annex 3;

(c) state any other cyber security industry standards over and above those set out in this Schedule which are applicable to the Services;

(d) state all applicable law which relates to the security of the Services; and

(e) how the Service Provider will comply with any other security requirements TfL may reasonably request from time to time.

When the Security Management Plan is approved by TfL the approved plan will replace the Outline Security Management Plan in Annex 1.

14.3 The Service Provider shall review and update the Security Management Plan at least annually and as required in response to:

(a) changes to the Cyber Security Standards;

(b) emerging changes in Good Industry Practice;

(c) any relevant Operational Change or Variation and/or associated processes;

(d) any new perceived or changed security threats; and

(e) any reasonable request by TfL.

14.4 The Service Provider shall submit any amendments to the Security Management Plan for Approval by TfL in accordance with the variation procedure set out in this Agreement

15. INFORMATION SECURITY MANAGEMENT SYSTEM

15.1 The Service Provider shall develop, implement, operate, maintain the ISMS and shall within fifteen (15) Working Days of the Effective Date submit a draft ISMS to TfL to assure. The Service Provider

shall ensure that the ISMS includes the Security Incident Management Process, dealing with, among other matters, Security Incident management.

15.2 The ISMS shall, unless otherwise specified by TfL in writing, be designed to protect all aspects of:

(a) the Services;

(b) all processes associated with the delivery of the Services; and

(c) TfL Sites, the Service Provider Solution and any information and Data (including TfL Confidential Information and TfL Data) to the extent used by TfL or the Service Provider in connection with this Agreement.

15.3 The Service Provider shall make any document referenced in the ISMS available to TfL upon request.

15.4 If the investigation of a Security Incident reveals weaknesses or flaws in the ISMS, then any change to the ISMS to remedy the weakness or flaw shall be submitted to TfL for approval in accordance with the Variation procedure set out in this Agreement for the avoidance of doubt, if a change needs to be made to the ISMS to address an instance of non-compliance with the Security Management Plan or security requirements, the change to the ISMS shall be at no cost to TfL.

15.5 The ISMS will be fully reviewed in accordance with ISO/IEC 27001 by the Service Provider at least annually, or from time to time as agreed with TfL, in response to:

(a) changes to Good Industry Practice;

(b) any relevant Operational Changes or Variations or proposed Operational Changes or Variations to the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by TfL.

15.6 The Service Provider shall provide the results of such reviews to TfL (together with such related information as TfL may reasonably request) as soon as reasonably practicable after their completion. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that affect the ability to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

16. COMPLIANCE WITH ISO/IEC 27001

16.1 The Service Provider shall obtain certification from a UKAS registered organisation of the ISMS to ISO/IEC 27001 for any aspects of the business that is necessary to support the Services. The Service Provider shall obtain such certification within twelve (12) months of the Effective Date and shall maintain such certification throughout the Term.

16.2 If certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27001, the Service Provider shall promptly notify TfL of this.

16.3 Without prejudice to any other audit rights set out in this Agreement TfL may carry out, or appoint an independent auditor to carry out, such regular security audits as may be required in accordance with

Good Industry Practice in order to ensure that the ISMS maintains compliance with the principles and practices of ISO/IEC27001.

16.4 If on the basis of evidence provided by such audits, TfL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Service Provider, then TfL shall notify the Service Provider of the same and the Service Provider shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such non-compliance as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement.

17. APPROVED PRODUCTS

17.1 The Service Provider shall ensure that all Service Assets providing security enforcing functionality are certified under the CESG Commercial Product Assurance (CPA) Scheme, to the appropriate grade, as defined with Annex 3 “Security Requirements”, provided that relevant certified products are available in the market.

17.2 If a product is not assured under the CPA scheme, TfL reserves the right to require bespoke assurance of that product under a recognised scheme such as CESG Tailored Assurance Service (CTAS).

ANNEX 1 – OUTLINE SECURITY MANAGEMENT PLAN/SECURITY MANAGEMENT PLAN

[redacted]

ANNEX 2 – OUTLINE RISK MANAGEMENT PROCESS

[redacted]

•

ANNEX 3 – SECURITY REQUIREMENTS

[redacted]

ANNEX 4 – CONFIGURATION MANAGEMENT OF SERVICE ASSETS

[redacted]

ANNEX 5 – LIST OF RELEVANT POLICIES

TO BE PROVIDED BY TFL UPON REQUEST

- **Network Security Policy** defines the requirements for securing TfL networks as well as the information and network specific devices on them.

- **System Access Control Policy** defines the requirements for managing user and system account access to applications and technology such as allowing them to sign in to OneLondon or SAP.

- **Cyber Security Incident Management Policy** defines how we will handle cyber security incidents and the requirements for reporting and managing those incidents.

- **Malware Prevention Policy** defines the requirements for helping to prevent malware (malicious software e.g., computer viruses) from infecting our systems and networks.

- **Security Logging, Monitoring and Audit Policy** details the requirements for security logging and monitoring of access to our technology and data and the audit capabilities.

- **Removable Media Policy** details the requirements for using removable media such as USBs, CDs or portable hard drives.

- **Home and Mobile Working Cyber Security Policy** details the requirements for allowing and supporting secure home and mobile working.

- **Third Party Cyber Security Policy** defines the rules governing how the security of third-party custodians of TfL information, technology and third party connections to TfL systems will be ensured.

- **TfL Information Security Classification Standard** details the information security classification scheme covering information and records, in all formats, and the minimum requirements for managing such information

- **10 Steps to Cyber Security -** https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

- **Cyber Essentials Scheme https://www.gov.uk/government/publications/cyber-essentials-scheme-overview**

- **Security Patching Standard** details the requirements for applying security-related updates ('security patches') in order to help secure TTL systems and applications in line with the secure builds and configurations policy.

Operations Technology Cyber Security Standard describes the cyber security requirements for operational technology assets throughout their li