SCHEDULE 2.3

STANDARDS

LOT 2

VERSION CONTROL

VERSION NUMBER	DATE	COMMENT
1.0	July 2021	Execution Version

CONTENTS

1. PURPOSE 1

2. CHANGES TO STANDARDS 1

APPENDIX 1 – STANDARDS 2

SCHEDULE 2.3 – STANDARDS

1. PURPOSE

1.1 This Schedule sets out the Standards for the purpose of this Agreement.

1.2 TfL shall provide the Supplier with copies of, or access to, the Standards that are controlled by TfL. The Supplier acknowledges that at the Effective Date all of the Standards set out in Appendix 1 have been made available to the Supplier.

2. CHANGES TO STANDARDS

2.1 Throughout the Term the Parties shall monitor and notify each other of any new or emergent policies or standards which could affect the performance of this Agreement including TfL's receipt of the Services.

2.2 Any changes to the Standards, including the adoption of any such new or emergent policy or standard, shall be agreed in accordance with the Change Control Procedure, provided that if there is an industry-led update, amendment or replacement of any Standard that is reasonably categorised as an industry standard, the Supplier shall comply with such updated, amended or replacement Standard at no additional cost to TfL.

2.3 Where TfL notifies the Supplier of any new or emergent policy or standard developed or introduced by TfL, the Supplier shall be responsible for ensuring that the potential impact on this Agreement (including on TfL's receipt of the Services) is explained to TfL (in a reasonable timeframe) prior to the implementation of the new or emergent policy or standard.

2.4 Where Standards conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier unless TfL requires or approves otherwise in writing.

APPENDIX 1 – STANDARDS

1. TfL STANDARDS

REF.	TITLE	ISSUE NUMBER / DATE
Information Governance		
P113	Information Access Policy	V2/May 2012
P114	Information and Records Management Policy	V2/April 2012
P115	Information Re-use Policy	V2/April 2012
P116	Information Security Policy	V2/May 2012
P118	Corporate Archives Policy	V1/May 2012
P023	Privacy and Data Protection Policy	A2/May 2018
P043	Policy on the Disclosure of Personal Data to the Police and Statutory Enforcement Agencies	V2/March 2015
R2973	TfL Information and Records Disposal Schedule	A2/May 2018
Technology and Data standards		
G2405	Firewall selection and deployment	A1/December 2018
G2406	Firewalls Security	A1/December 2018
G2408	Encryption and Cryptography	A1/December 2018
G2409	Blocked Websites	A1/January 2018

REF.	TITLE	ISSUE NUMBER / DATE
G2410	Blocked Files	A1/January 2018
G2411	Authentication Secrets	A1/January 2018
P123	Cyber Security Risk Management Policy	A1 / March 2018
P124	Secure Builds and Configurations	A2/February 2018
P125	Network Cyber Security Policy	A2/February 2018
P126	System Access Control Policy	A2/February 2018
P127	Cyber Security Incident Management Policy	A2/February 2018
P128	Malware Prevention Policy	A2/February 2018
P129	Security Logging, Monitoring and Audit Policy	A2/February 2018
P130	Removable Media Controls Policy	A2/March 2018
P131	Home and Mobile Working Policy	A2/March 2018
P132	Third Party Cyber Security Policy	A2/March 2018
S1735	System Access Control Standard	A2/March 2018
S1736	Network Cyber Security Standard	A2/March 2018
S1737	Secure Builds and Configurations Standard	A2/March 2018
S1738	Security Logging, Monitoring and Audit Standard	A2/March 2018

REF.	TITLE	ISSUE NUMBER / DATE
S1739	Security Patching Standard	A2/March 2018
S1740	Cryptography Standard	A2/March 2018
S1741	Cloud Cyber Security Standard	A2/March 2018
S1744	Operational Technology Cyber Security Standard	A1/Apr 2017
S1745	Cyber Security Vulnerability Management Standard	A1 / March 2018
S1746	Cyber Security Testing Standard	A1 / March 2018
S1747	Physical Security of IT Equipment Standard	A1/March 2018
S1748	Wireless Networks and Communications Security Standard	A1/March 2018
S1749	Secure Application and Web Development Standard	A1/March 2018
S1744	Operational Technology Cyber Security	A1/April 2017
S1782	Information Security Classification Standard	02/09/2016
R2927	Cyber Security Framework Reference	A2/February 2018
	Single Sign On Guidelines	V1/January 2014
	Configuration Management Guidelines	V1/November 2013
	Incident Management Guidelines	V1/November 2013
	Release Management Guidelines	V1/November 2013

REF.	TITLE	ISSUE NUMBER / DATE
	Change Management Guidelines	V1/November 2013
	Service models	V1/November 2013
	Security and Risk Management	V2/June 2015
	Metadata and Metatags	V1/November 2013
	Digital experience principles	V1/November 2013
	Accessibility	V1/November 2013
	Putting users first	V1/November 2013
	Personas	V1/November 2013
	User Testing and Research	V1/November 2013
	Benchmarking and Analytics	V1/November 2013
	Information Architecture principles	V1/November 2013
	Design Style Guide	V3/October 2014
	Brand Iconography	V1/February 2014
	Digital Photography	V1/January 2014
	PDFs and attachments	V1/February 2016
	Short URL and domain name	V4/July 2014

REF.	TITLE	ISSUE NUMBER / DATE
	Digital Content	V4/January 2014
PUB17_038	Editorial Style Guide	October 2017
	Go live acceptance criteria	V1/November 2013
	Service acceptance criteria	V1/November 2013
	User acceptance testing and sign off	V1/December 2013
	Guide to Testing requirements	V1/November 2013
	Compatibility testing	V1/December 2013
	Development testing	V1/November 2013
	Functional testing	V1/November 2013
	Integration testing	V1/November 2013
	Operational acceptance testing	V1/November 2013
	Penetration testing	V1/November 2013
	Performance testing	V1/November 2013
Corporate Governance		
P021	Enterprise Risk Management Policy	A2/May 2019
P078	TfL Code of Conduct	A8/October 2018

REF.	TITLE	ISSUE NUMBER / DATE
P079	TfL's Resilience Management Policy Framework	A2/May 2019
P105	TfL Anti-Fraud and Corruption Policy	A2/November 2018
R2974	TfL Information and Records Disposal Schedule (for Property and Assets)	March 2018
Health, Safety and Wellbeing		
P133	TfL Health, Safety and Environment Policy	A4/August 2019
P101	Safety and Wellbeing Policy	A5/September 2018
Human Resources		
P049	Acceptable use policy (computer facilities, assets and electronic communications technologies)	A3/May 2018
P087	Bullying and Harassment Policy and Procedure	A4/May 2019
P082	Drugs/Alcohol Policy and Procedure	A2 November 2016
P092	Equality and Inclusion Policy	October 2010
P102	Social Media Policy	A1/July 2015
Style and Design		
P106	Accessible Communications Policy	August 2014
Issue16	Advertising and Services Information Standard	July 2016
Issue7	Basic Elements Standard	September 2018

REF.	TITLE	ISSUE NUMBER / DATE
Issue4	Colour Standard	May 2016
Issue2	Digital Displays	July 2016
Issue3	TfL Branding Standard for Licensed Private Hire Operators	April 2016
TPH Business Rules and other TPH policies		
	TPH - Business Rules 01 - Supplier Contact Centre	
	TPH - Business Rules 02 - TfL Contact Centre	
	TPH - Business Rules 03 - Customer Account	
	TPH - Business Rules 05 - Mandatory Requirements	
	TPH - Business Rules 09 - Exemptions	
	TPH - Business Rules 10 - Vehicles	
	TPH - Business Rules 12 - Payments and Refunds	
	TPH - Business Rules 13 - Post Licensing	
	TPH - Business Rules 14 - Appeals	
	TPH - Business Rules 15 - Scanning	
	TPH - Business Rules 16 - Printing	
	TPH-Appendix01-Policy-Information Compliance	

REF.	TITLE	ISSUE NUMBER / DATE
	TPH-Appendix02-Policy-Data Retention Electronic Documents Policy	
	TPH-Appendix12-Policy-Returns Refunds policy	
	TPH-Appendix17-Policy-Vehicle Licensing Inspection Manual	
	TPH-Appendix23-Information-Vehicle Inspection Types and Definitions	

2. OTHER STANDARDS

REF.	TITLE	ISSUE NUMBER / DATE
ISO 9001:2015	Quality Management Systems – Requirements https://www.iso.org/standard/62085.html	September 2015
ISO/IEC 27001:2013	Information Security Management System https://www.iso.org/standard/54534.html	October 2013
	Government Digital Services guidelines for API technical and data standards https://www.gov.uk/guidance/gds-api-technical-and-data-standards	February 2018
	Digital accessibility testing standard https://tfl.gov.uk/info-for/suppliers-and-contractors/digital-design-toolkit/digital-accessibility-testing-standard	

REF.	TITLE	ISSUE NUMBER / DATE
	Open Web Application Security Project (OWASP) secure coding guidelines http://www.w3.org/TR/WCAG21	
ISO/IEC 26514:2008	Guidelines for the design and development of software user documentation for computer-based application systems as part of the life cycle processes	
S EN 60950-1:2006+A2:2013B	Specification for safety of information technology equipment, including electrical business equipment	
ISO 22301	Best-practice framework for implementing an optimised BCMS (business continuity management system)	
ISO 22313	Business Continuity Management Guidance	
E-GIF	E- Government Inter-Operability standards	
	Payment Card Industry Data Security Standard (PCI DSS)	3.2.1/May 2018
	International Financial Reporting Standards (IFRS)	
ISA 402	Audit Considerations Relating to an Entity Using a Service Organization	December 2010
ISAE 3402	Assurance Reports on Controls at a Service Organisation	December 2009