# schedule 4

# STANDARDS

1. **INTRODUCTION**
   1. Should any of the policies or standards for the purposes of this schedule be amended in accordance with the provisions of this agreement (including where version numbers are updated) then such amendments shall be reflected by the parties in the Policy Document Control Sheet in accordance with the controlled document process notified by the Authority to the Supplier from time to time.
   2. The Supplier shall comply with the Standards.
   3. A change to an Authority’s Specific Standard shall be deemed to be a general Change in Standards to the extent it arises as a consequence of a change to any of the General Standards referred to below provided.
2. **GDPR AND DATA PROTECTION**
   1. The Supplied System shall store data in order to meet the requirements of the UK GDPR in relation to the use and storage of personal data.
   2. All components of the Supplied System must have an approved DPIA to ensure compliance with the Authority’s policies for use of data.
   3. The Supplier shall confirm the extent of personally identifiable data that will be held on the Supplied System.
   4. The Supplier shall confirm that the Supplied System complies with Data Subject Rights, in particular that:
      1. all personally identifiable data held on the system applicable to a single individual can be gathered together in a simple to understand report;
      2. where appropriate, such personally identifiable data can be updated and changed;
      3. in the event of errors in such data being suspected or found, the data concerned can be frozen whilst an investigation takes place; and
      4. if errors are confirmed, these can be corrected.
3. **GENERAL STANDARDS**
   1. All Hardware supplied shall provide fluid and dust ingress protection to BS EN 60529:2004 (identical to ANSI/IEC 60529:2004 and EN 60529:2004) IP rating of at least 54 (in normal usage configuration) providing protection against dust with limited ingress (no harmful deposit) and against sprays from all directions with limited ingress permitted. This requirement is to protect the equipment against accidental damage from the bus-wash or other environmental hazards.
   2. All electrical Hardware supplied shall comply with the European EMC Directive 2004/108/EC Electromagnetic Compatibility for the generation by the equipment of electromagnetic radiation and conducted electrical interference, such that the Hardware does not disrupt or interfere with any radio equipment, radio system or unrelated equipment or system and for immunity from conducted and radiated electrical interference likely to be experienced in the operating environment. Including at the location where the equipment will be installed including susceptibility to radiation from current and future radio equipment and systems.
   3. The Supplier shall provide evidence of compliance, as required by this agreement.
   4. All Hardware supplied shall have been prior tested to meet all relevant requirements of the National and European standards set out above and any others which the Supplier has found to be relevant.
   5. All Hardware supplied shall be certified as EMC interference immune and having no particular date dependent failure modes.
   6. All Hardware supplied shall have received all relevant Type Approvals and the Authority shall be indemnified against any non-compliances statutory or otherwise.
   7. The Supplier shall maintain continued compliance with all appropriate health and safety related standards at no cost to the Authority.
   8. Certificates confirming compliance with National and European International standards shall be delivered to the Authority before Testing commences.
   9. The on-bus AVA system should be an E-Mark product with the UNECE R10 Approval number to allow the terminals to be fitted at the time of vehicle manufacture.
   10. The Supplied System (including AVAs) should have regulatory compliance for the products sold in Great Britain and should be an UKCA (United Kingdom Conformity Assessed) marked product. Using the UKCA marking - GOV.UK (www.gov.uk) provides more information on UKAS product certification.
   11. The on-bus AVA system should be capable of interfacing to on-bus AVL system provided to the Authority by a third party service provider to obtain the service information, location, date and time information in compliance with ITxPT S02 Onboard Architecture Specification, Section 3 Table 4:
       1. Part 01: Module Inventory Service;
       2. Part 02: Time Service; and
       3. Part 03: GNSS Service.
   12. The Supplied System shall comply with the:
       1. IEEE 802.3 Ethernet standard;
       2. IEEE 802.1x port-based Network Access Control (PNAC) standard; and
       3. IEEE 802.11a/b/g/n, IEEE802.11ac (WiFi5), and IEEE 802.11ax (WiFi6) established and emerging wireless standards operating in the 2.4GHz and 5GHz spectrums.
4. **SECURITY**
   1. The Supplier shall hold ISO 27001 certification (see also Schedule 6 (Security Management Plan)).
   2. The Supplier's security management system shall meet the Cyber Essentials security standard or any such equivalent or improved standard from time to time.
   3. The Supplier shall at its own cost maintain its ISO 27001 and Cyber Essentials certification (or in the case of Cyber Essentials, any such equivalent or improved certification from time to time) via annual audits during this agreement. The Supplier shall make the results of each audit available to the Authority within five Working Days after receipt of the audit results.
5. **AUTHORITY SPECIFIC STANDARDS** 
   1. P01 Information Security Policy
   2. P02 Information Systems Security Audit Policy
   3. P03 IS Disaster Recovery and Security Incident Response Policy
   4. P04 IS Wireless Policy
   5. P05 IS Operational Policy
   6. P06 IS Acceptable Policy
   7. P07 IS Third Party and Service Provider Policy
   8. P08 IS Classification Policy (Credit Card Data)
   9. P09 IS Key Management Policy
   10. P10 IS Physical Security Policy
   11. P11 IS Systems and Application Development Policy
   12. P12 Penetration Testing Policy
   13. Security Incident Response Plan

*IS Policies*

* 1. 001 IS Acceptable Use Policy
  2. 002 IS Access Control Policy
  3. 003 IS Asset Management Policy
  4. 004 IS Back-up Policy
  5. 005 IS Change Management Policy
  6. 006 IS Classification Policy
  7. 007 IS Compliance Policy
  8. 008 IS Disposal of Confidential Waste
  9. 009 IS Electronic Communications
  10. 010 IS Email Policy
  11. 011 IS Encryption Policy
  12. 012 IS Guest Policy
  13. 013 IS HR Information Security Policy
  14. 014 IS Incident and Response Policy
  15. 015 IS Management and Control of Mobile Communications
  16. 016 IS Mobile Device Usage Policy
  17. 017 IS Network Control Policy
  18. 018 IS Network Security Management
  19. 019 IS Operations Policy
  20. 020 IS Physical Security Policy
  21. 021 IS Remote Policy
  22. 022 IS Removable Media Policy
  23. 023 IS Systems and Administrative Password Policy
  24. 024 Security Patching Policy
  25. 025 System Acquisition Development and Maintenance Policy
  26. 026 IS Technology Usage Policy
  27. 027 IS Test Security Policy
  28. 028 IS Third party Policy
  29. 029 IS Virus and Anti-Virus Policy
  30. 030 IS VPN Policy
  31. 031 IS Wireless Access Policy

*Other Policies*

* 1. Asset Management Policy
  2. Code of Conduct
  3. Anti-Bribery and Corruption Policy
  4. Anti-Fraud Policy Statement
  5. Anti-Money Laundering Policy
  6. Recovery of Assets and Sanctions Policy
  7. Data Protection Policy
  8. TfGM Summary of Energy and Carbon Strategy 2018 to 2021
  9. Transparency and Open Data Policy
  10. Diversity and Inclusion Policy