Schedule 8.4 – Document Management

CHANGE HISTORY

Version	Description	Author	Document Number
5.0	Execution version	TfL	75252223.12

Contents

1 Introduction

1.1 This Schedule sets out:

(a) the obligations of the Concessionaire to provide the Documents;

(b) the requirements for the Concessionaire to provide and maintain:

(i) the Document Management Plan, as described in Paragraph 2.1;

(ii) the Document Management System, as described in Paragraphs 2.5 to 2.14; and

(iii) the Document Register, as described in Paragraphs 2.15 and 2.16; and

(c) the process of Document exchange and review as described in Paragraph 4.

1.2 The objectives of this Schedule are to ensure that:

(a) Documents will be established, maintained and stored in a consistent manner that will allow information to be made available to TTL as required by Clause 13 (Records, Reports and Audits);

(b) Documents are stored in a secure manner to ensure the on-going confidentiality of the Documents and the security of the Services;

(c) changes to Documents are controlled and subject to appropriate Approval and Assurance by TTL; and

(d) Documents are shared in a structured and controlled manner to support the delivery of the Services.

1.3 In addition to the Concessionaire's obligation to manage Documents in accordance with this Schedule, the Concessionaire shall ensure that all Records which are not Documents are managed and stored in accordance with Good Industry Practice and the Information and Records Management Policy referred to in Schedule 2.3 (Standards) to enable the efficient and effective delivery of the Services including the Concessionaire's obligations in relation to Audits. Such storage and management shall include version control, security management, the management of transmittals and records management including retention and disposal policies.

Documents to be Submitted by the Concessionaire

1.4 The Concessionaire shall prepare, submit, and maintain:

(a) the Document Management Plan;

(b) the Document Register;

(c) the Documents;

(d) the Reports;

(e) the Records; and

(f) any documented information required to be submitted by the Concessionaire to TTL under this Agreement,

in accordance with the requirements of this Schedule.

1.5 The Concessionaire shall prepare all Documents required by this Agreement in accordance with the provisions of this Schedule and any relevant Standards.

2 Document Management

Document Management Plan

2.1 The Document Management Plan is set out at Annex 2 (Document Management Plan).

2.2 The Concessionaire shall ensure that notwithstanding any amendments made in accordance with Paragraph 2.17, the Document Management Plan always sets out:

(a) the principles that govern (as relevant to the specific Document) the planning, preparation, production, classification, indexing, checking, submission, distribution, updating, use, storage, traceability, retrievability and security controls of all Documents;

(b) a document classification system and the standards the Concessionaire shall adopt for each classification;

(c) details of the Concessionaire's document management strategy, including:

(i) the Concessionaire's approach to liaising with TTL in relation to Documents;

(ii) details of all the Concessionaire's processes to ensure protection, security, sharing and storage; and

(iii) a list of the software used to generate and manage Documents;

(d) details of the processes the Concessionaire will use to review and update Documents as required when Change is undertaken, ensuring that each Document clearly states which other Documents it supersedes;

(e) a document retention schedule setting out which Documents will be retained and for how long in accordance with the provisions of Clause 13 (Records, Reports and Audits);

(f) details of the Document Management System (including user roles, responsibilities and permissions, audits, logs and access management); and

(g) details of the Document Register.

2.3 The Concessionaire and TTL shall work together to identify those Documents which shall be security classified in accordance with Government Security Classifications and apply the appropriate process as specified in the Security Management Plan.

2.4 The Concessionaire may not change any aspect of its document management strategy described at Paragraph 2.2(c) that has or is reasonably likely to have a material impact on TTL's management of this Agreement without the prior written agreement of TTL.

Document Management System

2.5 The Concessionaire shall adopt an efficient Document Management System which conforms to Good Industry Practice.

2.6 The Concessionaire shall operate the Document Management System and provide details of the functionality, operation and use of such system to TTL upon request. The Document Management

System shall include procedures for managing Documents. The classification details of the Documents shall be included in the Document Management Plan.

2.7 Where there is more than one (1) version of a Document then the Concessionaire shall implement a document control system and record details of the status of all versions of a Document and clearly identify the most current version within the Document Management System. The Concessionaire shall ensure that Documents that are required to be Approved or Assured by TTL are marked with an appropriate designation in the Document Management System.

2.8 The Concessionaire shall ensure that the Document Management System shall enable the controlled electronic management of working Documents between the Parties for the purpose of review and comment in relation to the delivery of the Services in accordance with the applicable Government Security Classifications.

2.9 The Concessionaire shall ensure that the Document Management System shall, where appropriate, as a minimum:

(a) enable TTL Personnel and third parties as authorised by TTL, to easily access, mark-up and add comments to Documents;

(b) enable remote access for TTL, any member of the TfL Group and third parties nominated by TTL from time to time, through the world wide web using a browser-based interface;

(c) classify Documents according to the Government Security Classifications;

(d) automate the request, review, Approval and Assurance processes for Documents;

(e) enable supporting and referenced Documents to be accessed on the same system;

(f) record and enable the audit of all Document changes through an immutable audit trail;

(g) where required:

(i) enable a user of the Document Management System to have a Document 'checked out' such that other users cannot alter the Document; or

(ii) provide read-only access to Documents;

(h) make Documents easy to find by providing flexible search options;

(i) use permissions to control access to Documents, including role or user-based permissions (for example, if TTL requires an authorised third party to access a specific sub-set of Documents, role or user-based permissions shall be used to restrict the third party's access to that particular sub-set of Documents); and

(j) be backed-up on at least a daily basis and stored securely in such a manner that ensures availability of the Document Management System is not compromised during the Term and in accordance with Schedule 8.6 (Business Continuity and Disaster Recovery).

provided that only Paragraphs 2.9(b), 2.9(f), 2.9(g)(i), 2.9(i) and 2.9(j) shall apply to the CMDB.

2.10 The Concessionaire shall ensure that its Document Management System (and its CMDB system) complies with the provisions of Schedule 2.4 (Security Management).

2.11 The Concessionaire shall operate the Document Management System (and its CMDB system) to ensure that, at a minimum:

(a) all data that relates to Documents in the Document Management System and data within the CMDB is encrypted;

(b) no data (including all back-ups of such data) is hosted, stored or transmitted in or to Restricted Countries without the prior consent of TTL;

(c) user access is maintained on the principle of 'least privilege' so that users of the Document Management System shall only be able to access the information that is deemed necessary for their particular purpose, and the details of how that principle is applied shall be included in the Document Management Plan; and

(d) TTL, any members of the TfL Group and third party access to the Document Management System is restricted to devices on TTL-approved public IP addresses.

2.12 Prior to implementation the Concessionaire shall test the proposed Document Management System in accordance with the Test Strategy to ensure that it meets TTL's requirements and the requirements set out in this Schedule.

2.13 The Concessionaire shall regularly, at least once every Contract Year, test the Document Management System back up and recovery procedure.

2.14 In respect of any Documents that require Approval by TTL, the Concessionaire shall ensure that the Document Management System captures and records all necessary metadata to verify that the Documents have been Approved by suitably authorised TTL Personnel.

Document Register

2.15 The Concessionaire shall maintain (on a Near Real Time basis) an accurate Document Register that allows Documents to be sorted, selected and issued to TTL by any combination of the following:

(a) unique reference;

(b) dates (e.g. of issue, of revision);

(c) revision number;

(d) title;

(e) subject matter based on the use of key words;

(f) issue number;

(g) status (e.g. draft, submitted, production etc.);

(h) originating organisation and author; and

(i) file type.

2.16 The Concessionaire shall retain details of superseded Documents (with the exception of the CMDB) and a record of the associated superseding Documents together with an audit trail.

Review and Updating

2.17 The Concessionaire shall review and, if necessary, update the Document Management Plan on each anniversary of the Effective Date during the Term or more frequently as required.

2.18 The Concessionaire shall discuss all proposals to upgrade or introduce any new document creation or management software with TTL at least six (6) months prior to the planned implementation date and:

(a) the Concessionaire shall not unreasonably refuse to take into account TTL's comments in relation to the implementation timing of any such proposals; and

(b) shall reimburse to TTL all costs TTL reasonably incurs as a result of the introduction of such upgraded or new software.

2.19 The Concessionaire shall maintain the Document Management System and content of the Document Register as current.

2.20 The Concessionaire shall report progress on any issues arising from the Document Management Plan, Document Management System, CMDB system and Document Register in the Performance Monitoring Report (PMR1) and shall discuss the same at the Monthly Operational Meeting required by Schedule 8.1 (Governance).

2.21 If an incident occurs in respect of the Document Management System or the CMDB, the Concessionaire shall resolve and report on such incident in accordance with the Concessionaire's incident management process.

3 Documents

3.1 The Concessionaire shall:

(a) retain all Documents in electronic formats unless hard copy format is requested by TTL. The Concessionaire shall maintain back-ups of all Documents in a manner which ensures easy, secure and complete recovery in the event that a restore is required.

(b) make available all Documents in electronic format via the Document Management System (except for the CMDB which shall delivered through the IT service management (ITSM) system) and within such timeframes as specified in this Agreement or otherwise reasonably requested by TTL. Documents for review shall be made available in their native electronic format and any alternative electronic or hard copy format reasonably required by TTL to enable review, mark-up and comment;

(c) ensure every Document (with the exception of the CMDB) displays an appropriate copyright statement and protective marking correctly reflecting its status in accordance with the Concessionaire's Security Management Plan;

(d) generate Documents in accordance with Good Industry Practice. When a Document is to be supplied to TTL for the first time then the Concessionaire shall discuss its proposed standard with TTL and incorporate TTL's reasonable comments;

(e) submit details of the standards it uses as part of its Document Management Plan;

(f) for Documents which contain sensitive security information such as usernames or login details, be able to provide such documents in redacted and unredacted forms;

(g) accompany any CAD drawing information transmitted in electronic format with details of the loading method, the files provided, the status of the files and the relevant symbol libraries; and

(h) create, share and store all Documents in a manner which enables TTL to easily produce legible copies suitable for viewing and printing in accordance with the Document Management Plan.

3.2 The Concessionaire shall ensure that procedures are in place to ensure that all Documents are clearly marked with their appropriate status code (for example 'draft' and 'for review') and are dated and signed as "checked and approved" by approved Concessionaire Personnel.

3.3 The Concessionaire shall implement procedures to ensure that all Documents issued to TTL shall be accompanied with a suitable Documents transmittal note or auditable electronic delivery receipt process in accordance with the provisions of the Submissions Procedure.

3.4 All versions of a Documents (with the exception of the CMDB) shall be clearly marked on the Documents and shall state clearly the reason and authorisation for the revision.

3.5 The Concessionaire shall ensure that the content and presentation of all Documents are of the appropriate level of quality and fit for its intended purpose, including in respect of clarity, structure, spelling and punctuation.

3.6 Without limiting any other provision in this Agreement, the Concessionaire shall implement processes to ensure that only virus-free electronic information is sent or stored in accordance with Clause 21 (Data and Security Requirements).

4 Submissions Procedure

Overview

4.1 The Concessionaire shall ensure that each Document is Approved or Assured by TTL as required under this Agreement. The Concessionaire shall ensure that the Document Register accurately records for each Document whether it is required to be Approved or Assured by TTL.

4.2 If a Document is required to be Approved by TTL, the relevant Document shall only be Approved pursuant to Paragraphs 4.4 and 4.5.

4.3 If a Document is required to be Assured by TTL, the relevant Document shall only be Assured pursuant to Paragraphs 4.6 and 4.7.

Approval

4.4 Each time the Concessionaire is required to submit a Document to TTL for Approval, the Concessionaire shall either (as directed by TTL):

(a) submit such Document to the relevant Governance Meeting (as indicated in the Document Register) for TTL to consider and, if appropriate, confirm in writing as Approved at the Governance Meeting (such confirmation to be recorded in the minutes of the meeting);

(b) follow the processes set out in Paragraphs 4.8 to 4.27 in relation to the submission and iteration of such Document; or

(c) submit such Document to TTL and comply with such process as TTL may (acting reasonably) specify in writing for the iteration and finalisation of such Document (including any such process set out elsewhere in this Agreement),

(such procedure being the "**Approval Submissions Procedure**").

4.5 Notwithstanding Paragraph 4.4, the Concessionaire shall take full account of all TTL's comments on each draft Document required to be Approved and such Document shall only be Approved when TTL confirms that this is the case in writing.

Assurance

4.6 Each time the Concessionaire is required to submit a Document to TTL for Assurance the Concessionaire shall either (as directed by TTL):

(a) submit such Document to the relevant Governance Meeting (as indicated in the Document Register) for TTL to consider and, if appropriate, confirm in writing as Assured at the Governance Meeting (such confirmation to be recorded in the minutes of the meeting);

(b) follow any procedure set out in any engineering standard or process as directed by TTL;

(c) follow the processes set out in Paragraph 4.8 to 4.28 in relation to the submission and iteration of such Document; or

(d) submit such Document to TTL and comply with such process as TTL may (acting reasonably) specify in writing for the iteration and finalisation of such Document (including any such process set out elsewhere in this Agreement),

(such procedure being the "**Assurance Submissions Procedure**" and together with the Approval Submissions Procedure, the "**Submissions Procedure**").

4.7 Notwithstanding Paragraph 4.6, the Concessionaire shall take full account of all TTL's comments on each draft Document required to be Assured (as applicable).

Submission and Iteration of a Document

4.8 The processes referred to in Paragraphs 4.4(b) and 4.6(c) are comprised of the following periods:

(a) preparation;

(b) submission;

(c) review;

(d) response;

(e) revision; and

(f) if relevant, deemed Assurance,

each of which is described in more detail in Paragraphs 4.9 to 4.28 below.

Preparation Period

4.9 During the preparation period, the Concessionaire shall prepare the relevant Document for submission to TTL for TTL's review.

4.10 The Concessionaire shall ensure that each Document is submitted with the following information:

(a) unique reference;

(b) dates (e.g. of submission, of revision);

(c) revision number;

(d) title;

(e) subject matter based on the use of key words;

(f) issue number;

(g) status (e.g. draft, submitted, production etc.);

(h) originating organisation and author;

(i) file type;

(j) a "response required by" date, where applicable;

(k) the purpose of the Document; and

(l) confirmation that the Document has been through all the necessary and appropriate Concessionaire checks and approvals.

4.11 The Concessionaire shall retain details of superseded Documents and a record of the associated superseding Documents together with an audit trail.

Submission Period

4.12 The Concessionaire shall make TTL aware by email to the address as notified by TTL and updated from time to time that a Document has been submitted in the Document Management System.

4.13 The Concessionaire shall promptly submit Documents in accordance with any deadline specified by TTL or agreed by the Parties in accordance with this Agreement or, if no deadline has been so specified or agreed, as soon as reasonably practicable.

4.14 Upon receipt of a notification that a Document has been submitted to the Document Management System, TTL shall review the sufficiency of the information received. TTL shall endeavour to respond to the Concessionaire within two (2) Working Days to:

(a) confirm the date and time of receipt of the Document by TTL; or

(b) request such further information that TTL considers is necessary to complete the review of the Document and the Concessionaire shall provide this further information to TTL within three (3) Working Days of TTL's request.

4.15 The further information process described in Paragraph 4.14(b) shall be repeated until TTL considers that it has sufficient information to review the Document and when TTL is satisfied then it shall confirm receipt of the Document to the Concessionaire in accordance with Paragraph 4.14(a).

Review Period

4.16 The review period shall commence upon confirmation by TTL of receipt of a Document in accordance with Paragraphs 4.14 to 4.15.

4.17 Once TTL has received all the necessary and requested information in accordance with Paragraphs 4.14 to 4.15, TTL shall review the Document and assess its compliance with the specified criteria and other relevant obligations set out in this Agreement.

4.18 During the review period the Concessionaire may supplement or may be requested by TTL to supplement the Document with presentations and workshops as appropriate.

Response Period

4.19 TTL shall respond to the Concessionaire with comments on the Document. TTL shall classify the comments as:

(a) critical;

(b) concerns;

(c) other comments; or

(d) recommendations.

4.20 TTL shall ensure that its comments are consistent with the Concessionaire's obligations under this Agreement, and in the case of critical comments shall state reasons why the Concessionaire's Document is not Assured or Approved as applicable.

4.21 TTL shall endeavour to:

(a) confirm the Document is Approved or Assured (as applicable); and/or

(b) provide the Concessionaire with its comments on the Document,

within ten (10) Working Days (or other period as may be agreed in writing between the Parties) of the date upon which TTL confirmed receipt of the Document pursuant to Paragraphs 4.14 and 4.15.

4.22 TTL may only withhold Approval or Assurance (as applicable) of a Document in the event TTL has comments which TTL has classified as either 'critical' or 'concerns'.

Revision Period

4.23 Notwithstanding Paragraph 4.21(a), the Concessionaire shall consider and respond to all of TTL's comments on the Document within ten (10) Working Days or other period as may be agreed in writing by the Parties.

4.24 The Concessionaire's response shall advise TTL of the action it will take in response to TTL's comments, which may be a combination of any of the following:

(a) incorporate the comments into the Document and submit the revised Document to TTL;

(b) provide a reasonable explanation for not incorporating TTL's comments into the Document;

(c) seek clarification; or

(d) provide such further information, presentations or demonstrations to provide assurance to TTL.

4.25 If, following TTL's Approval or Assurance (as applicable) at Paragraph 4.21(a), the Concessionaire:

(a) updates the Document and submits the revised Document to TTL pursuant to Paragraph 4.24(a); or

(b) amends the Document for any other reason,

the Document previously submitted to TTL will be the Approved or Assured (as applicable) Document until TTL Approves or Assures (as applicable) the revised Document.

4.26 At TTL's discretion, the Parties may repeat the process described in Paragraphs 4.12 to 4.25 until TTL is satisfied subject to Paragraph 4.22, that it has sufficient information to Approve or Assure (as applicable) the relevant Document.

4.27 The provisions of Paragraphs 4.12 to 4.25 shall apply again to any resubmitted Document provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

Deemed Assurance

4.28 In respect of the Documents which require Assurance (being those which have a tick in the "Assure" column in the table set out in Annex 1 (Document Register)), if TTL does not:

(a) request further information, presentations or workshops in accordance with Paragraph 4.14(b), 4.15, or 4.18; or

(b) provide comments to the Concessionaire in accordance with Paragraphs 4.19 to 4.21,

within ten (10) Working Days following confirmation by TTL of receipt of a Document required to be Assured in accordance with Paragraph 4.14, the provisions of Paragraphs 4.23 to 4.27 shall not apply and such Document shall be deemed to be Assured by TTL.

Annex 1 – Document Register

1.1 The Document Register agreed between the Parties as at the Effective Date is set out below.

Document Title	Reference	File Type	Template Reference	Initial Due Date	Frequency	Approve	Assure	Submissions Procedure
Remedial Adviser terms of engagement and start date	Clause 32.3(b)	.doc				✓		Schedule 8.4 Para 4.4
Step-In Plans	Clause 33.1			Within sixty (60) Working Days of the Effective Date or such longer period which TTL shall, in its absolute discretion, determine		✓		Schedule 8.4 Para 4.4
Step-Out Plan	Clause 33.8			Not less than twenty (20) Working Days prior to the Step-Out Date		✓		Schedule 8.4 Para 4.4
Works Instructions Document	Schedule 2.1 Requirement GRT3(i)	.doc		Within thirty (30) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Mobile High Level Design	Schedule 2.1 Requirement CMT1(a)			Within twenty (20) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Low Level Design – Station (Commercial Mobile) (Multiple)	Schedule 2.1 Requirement CMT1(k)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Mobile Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Tunnel Section (Commercial Mobile) (Multiple)	Schedule 2.1 Requirement CMT1(k)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Mobile Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Base Station Hotel (Commercial Mobile) (Multiple)	Schedule 2.1 Requirement CMT1(l)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Mobile Services Detailed Implementation Plan			✓	Schedule 8.4 Para 4.6
Low Level Design – ESN Annex 3 Location (Multiple)	Schedule 2.1 Requirement ESN1(a)	.doc		By Milestone Date specified in the Mobile Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Station (ESN) (Multiple)	Schedule 2.1 Requirement ESN1(a)	.doc		By Milestone Date specified in the Mobile Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Tunnel Section (ESN) (Multiple)	Schedule 2.1 Requirement ESN1(a)	.doc		By Milestone Date specified in the Mobile Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4

Document Title	Reference	File Type	Template Reference	Initial Due Date	Frequency	Approve	Assure	Submissions Procedure
Low Level Design – Base Station Hotel (ESN) (Multiple)	Schedule 2.1 Requirement CMT1(l)	.doc		By Milestone Date specified in the Mobile Services Detailed Implementation Plan			✓	Schedule 8.4 Para 4.6
Low Level Design – PoP (Fibre Services) (Multiple)	Schedule 2.1 Requirement FST1(b)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Fibre Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Station (Fibre Services) (Multiple)	Schedule 2.1 Requirement FST1(b)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Fibre Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Tunnel Section (Fibre Services) (Multiple)	Schedule 2.1 Requirement FST1(b)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Fibre Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Any Other Location (Fibre Services) (Multiple)	Schedule 2.1 Requirement FST1(b)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Fibre Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Streetscape Assets (Streetscape Services) (Multiple)	Schedule 2.1 Requirement SST1(b)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Streetscape Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Any Other Location (Multiple) (Streetscape Services)	Schedule 2.1 Requirement SST1(b)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Streetscape Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Low Level Design – Authentication Service (Public Wi-Fi)	Schedule 2.1 Requirement WFT1(a)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Public Wi-Fi Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Services Low Level Design – Internet Service (Public Wi-Fi)	Schedule 2.1 Requirement WFT1(a)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Public Wi-Fi Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4

Document Title	Reference	File Type	Template Reference	Initial Due Date	Frequency	Approve	Assure	Submissions Procedure
Low Level Design – Content Filter Service (Public Wi-Fi)	Schedule 2.1 Requirement WFT1(a)	.doc		By the relevant Milestone Date for the associated Milestones specified in the Public Wi-Fi Services Detailed Implementation Plan		✓		Schedule 8.4 Para 4.4
Security Management Plan	Schedule 2.4 Para 13.2	.doc		Within one hundred (100) Working Days of the Effective Date			✓	Schedule 8.4 Para 4.6
Concessionaire Software	Schedule 5	.doc	Schedule 5 Para 2		At least thirty (30) Working Days prior to each Annual Strategic Review Meeting		✓	Schedule 8.4 Para 4.6
Concessionaire Background IPR	Schedule 5	.doc	Schedule 5 Para 3		At least thirty (30) Working Days prior to each Annual Strategic Review Meeting		✓	Schedule 8.4 Para 4.6
Specially Written Software	Schedule 5	.doc	Schedule 5 Para 4		At least thirty (30) Working Days prior to each Annual Strategic Review Meeting		✓	Schedule 8.4 Para 4.6
Project Specific IPRS	Schedule 5	.doc	Schedule 5 Para 5		At least thirty (30) Working Days prior to each Annual Strategic Review Meeting		✓	Schedule 8.4 Para 4.6
Third Party Software	Schedule 5	.doc	Schedule 5 Para 6		At least thirty (30) Working Days prior to each Annual Strategic Review Meeting		✓	Schedule 8.4 Para 4.6
Third Party IPR	Schedule 5	.doc	Schedule 5 Para 7		At least thirty (30) Working Days prior to each Annual Strategic Review Meeting		✓	Schedule 8.4 Para 4.6

Document Title	Reference	File Type	Template Reference	Initial Due Date	Frequency	Approve	Assure	Submissions Procedure
Mobile Services Detailed Implementation Plan	Schedule 6.1 Para 3.1(a)	.mpp		Within thirty (30) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Fibre Services Detailed Implementation Plan	Schedule 6.1 Para 3.1(b)	.mpp		Within thirty (30) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Streetscape Services Detailed Implementation Plan	Schedule 6.1 Para 3.1(c)	.mpp		Within thirty (30) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Works Funded By Grants Detailed Implementation Plan	Schedule 6.1 Para 3.2	.mpp		Within thirty (30) Working Days of the option being exercised		✓		Schedule 8.4 Para 4.4
Public Wi-Fi Services Detailed Implementation Plan	Schedule 6.1 Para 3.3	.mpp		No later than 30 September 2022		✓		Schedule 8.4 Para 4.4
Updates to the Detailed Implementation Plans (Multiple)	Schedule 6.1 Para 4.1	.mpp			Not less than ten (10) Working Days prior to the beginning of each month	✓		Schedule 8.4 Para 4.4
Detailed Verification Activity Plan	Schedule 6.2 Para 2.3	.doc		Within thirty (30) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Updates to the Verification Activity Plan	Schedule 6.2 Para 2.6	.doc			Ad Hoc	✓		Schedule 8.4 Para 4.4
Detailed Test Strategy	Schedule 6.2 Para 4.3	.doc		Within sixty (60) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4
Updates to Test Strategy	Schedule 6.2 Para 4.7	.doc			Ad Hoc		✓	Schedule 8.4 Para 4.6
Test Plans	Schedule 6.2 Para 5.3	.doc	Schedule 6.2 Annex 3	Within twenty (20) Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the commencement of the relevant Testing			✓	Schedule 8.4 Para 4.6
Changes to Test Plan Templates	Schedule 6.2 Para 5.5	.doc			Ad Hoc	✓		Schedule 8.4 Para 4.4
Changes to Test Plans	Schedule 6.2 Para 5.6	.doc			Ad Hoc		✓	Schedule 8.4 Para 4.6
Changes to Reports	Schedule 8.1 Para 3.2	.doc			Ad Hoc		✓	Schedule 8.4 Para 4.6
Exit Plan	Schedule 8.5 Para 6.1	.doc		Within sixty (60) Working Days of the Effective Date		✓		Schedule 8.4 Para 4.4

Document Title	Reference	File Type	Template Reference	Initial Due Date	Frequency	Approve	Assure	Submissions Procedure
Updates to Exit Plan	Schedule 8.5 Para 6.4	.doc			Within first (1st) month of each Financial Year and within ten (10) Working Days of request following a Financial Distress Event	✓		Schedule 8.4 Para 4.4
Final form of the Exit Plan	Schedule 8.5 Para 6.5	.doc		Within twenty (20) Working Days after service of a Termination Notice or eighteen (18) months prior to Expiry Date		✓		Schedule 8.4 Para 4.4
BCDR Plan	Schedule 8.6 Para 1.1	.doc		Within forty (40) Working Days of the Effective Date			✓	Schedule 8.4 Para 4.6
BCDR Review Report	Schedule 8.6 Para 8.2	.doc			No later than thirty (30) Working Days prior to each Annual Strategic Meeting		✓	Schedule 8.4 Para 4.6

Annex 2 – Document Management Plan

1 Document Management Plan

1.1 This Document Management Plan sets out the Concessionaire's principles that govern the management of Documents.

Planning

1.2 The Concessionaire quality management system includes policies and procedures which underpin its Document Management System ("**DMS**") for the management of Documents (internal and external) for the Agreement. The principles of the DMS include:

(a) keeping documents organised
(b) controlling access to them
(c) enabling a better development and review process
(d) logging activity
(e) automatic record and document management e.g. reliable version control
(f) promotes collaboration and communication
(g) keep everyone up to date

1.3 The Concessionaire has several management plans to ensure effective management of its business. The plans provide the overall guidance to be used to perform the Agreement during the Term with references made to applicable communications policies, procedures and forms of the Concessionaire. For example, the Concessionaire's ultimate parent company has a global crisis management plan. Each operating business has a Business Continuity and Disaster Recovery Plan (BCDR). Detailed Business Continuity Plans underpin the BCDR which are reviewed periodically to an agreed schedule.

1.4 In addition to the plans included in the Document Register the Concessionaire will produce other plans in preparation to design, test and operate the Services. This will include:

(a) TfL File Plan (this will align with the Document Register). The draft File Plan for TCP documents is in the Annexes
(b) Service management plan
(c) Service asset and configuration management plan
(d) Audit plans (various)

Preparation

1.5 The Concessionaire has defined the Document Management file plan content and filing structure and meta data. The definition is based on Pathway to help understanding and align with TTL.

1.6 The required information for each Document will be provided when submitted, to comply with the requirements set out in Paragraphs 4.10(a) to 4.10(l).

Production

1.7 Designated templates are to be used for the development of any Document to ensure consistency and apply a quality management framework. Templates are available in the Concessionaire document portal on the Concessionaire's intranet. TTL-specific templates will be held in the TTL library.

1.8 Within the templates there are compulsory headings and then areas where the author can change as required. These are indicated within each template. Draft documents will be a minor version and watermarked with Draft. The Concessionaire can manage visibility of drafts to a different set of users

i.e. an operations person can only see major versions (approved) of processes. Meta data is assigned to all Documents used for sorting and searching e.g. document type or category.

Classification

1.9 Document classification is designed to ensure that access to information is correctly managed and safeguarded to a proportionate level throughout its lifecycle, including creation, storage, transmission and destruction.

1.10 To apply the correct classification, the document author or nominated owner of the information will conduct a damage or harm test. This considers the likely impact or consequences if the information were to be compromised, by assessing the information against the criteria for each protective marking.

1.11 The Concessionaire will use its Company Information Security Classification Policy for guidance; this aligns with TTL and government policy.

Indexing

1.12 The Concessionaire's DMS is SharePoint Online; this supports indexing of documents and the use of meta data to find and retrieve documents quickly and easily.

Checking

1.13 Documents will be checked before they are submitted to TTL for approval or assurance.

Low Level Design 3 levels of assurance

1.14 Review 1 is an internal review carried out by the author against a checklist.

1.15 Review 2 is carried out by the relevant subject matter expert. This may be a peer, line manager or other SME.

1.16 Review 3 is carried out by the design authority. A design check certificate is issued by the person compiling the document pack.

1.17 This level of assurance is applied to all Concessionaire Documents, whether for internal use or shared with TTL.

Submission

1.18 The Concessionaire will implement procedures to ensure that all Documents issued to TTL will be accompanied with a suitable Documents transmittal note or auditable electronic delivery receipt process in accordance with the provisions of the Submissions Procedure.

1.19 Using Exchange Online (the email platform within Office 365), and SharePoint Online the Concessionaire will automate tracking of email records and filing them in SharePoint, therefore providing an audit trail of when Documents are submitted.

Low Level Design (LLD) submission

1.20 The LLD Pack after the Concessionaire design authority approval, will be submitted via TTL's contractual document workflow toolset, Asite, which is 'New Engineering Contract' (NEC) compliant and coded to TTL's document naming convention for submission.

Distribution

1.21 Documents will be published in the DMS. The Concessionaire will manage distribution by granting access to the relevant libraries or folders to named individuals at TTL.

Updating

1.22 All controlled Documents will have a review date to ensure they are maintained and checked to ensure they remain applicable to the Services and compliant with legislation. SharePoint has a

version history of all Documents. If an approved Document is no longer required, it will be noted in the Document history within the Document and part of the meta-data. Documents will be retained in line with any relevant legislation and Annex 2B (UK Document and Personal Data Retention and Disposal Policy).

1.23 The review date will be held in the meta data, allowing the Concessionaire to track and progress reviews.

1.24 Changes to Documents will be reviewed and updated in line with the complexity of the change as described in the change process in table 4. The revision history in the Document will clearly state which other Document(s) it supersedes.

Use

1.25 The DMS will be used by all approved teams and individuals that require access to Documents to carry out their role and responsibilities under the Agreement. TTL will have access to Documents agreed in the Document Register. The Concessionaire suppliers will have access only to Documents required for the assigned work.

1.26 Access control will be managed by the Concessionaire's Document controller. The controller may be a dedicated role or a team with assigned responsibilities.

Storage

1.27 The storage solution will be appropriate for the type of data. Storage and management will include version control, security management, the management of transmittals and records management including retention and disposal policies. Microsoft Office 365 (including SharePoint online) is the primary document management solution.

1.28 Other IT systems are used in the Concessionaire e.g. for WHS or Personal Information. The use of other application native document management solutions will be assessed case by case depending on the processes and requirements. The assessment will include data held in OSS tools e.g. events in SolarWinds.

1.29 Records will have a defined retention period and when no longer required will be disposed of according to regulations and Annex 2B (UK Document and Personal Data Retention and Disposal Policy).

Traceability

1.30 The Concessionaire's tools and processes will enable easy traceability of documents and audit trail of Document creation, access, modification, approval and submission. All Documents in SharePoint have a version history which shows who and when modifications have been made. Comments can be added against status changes for approval / sign-off.

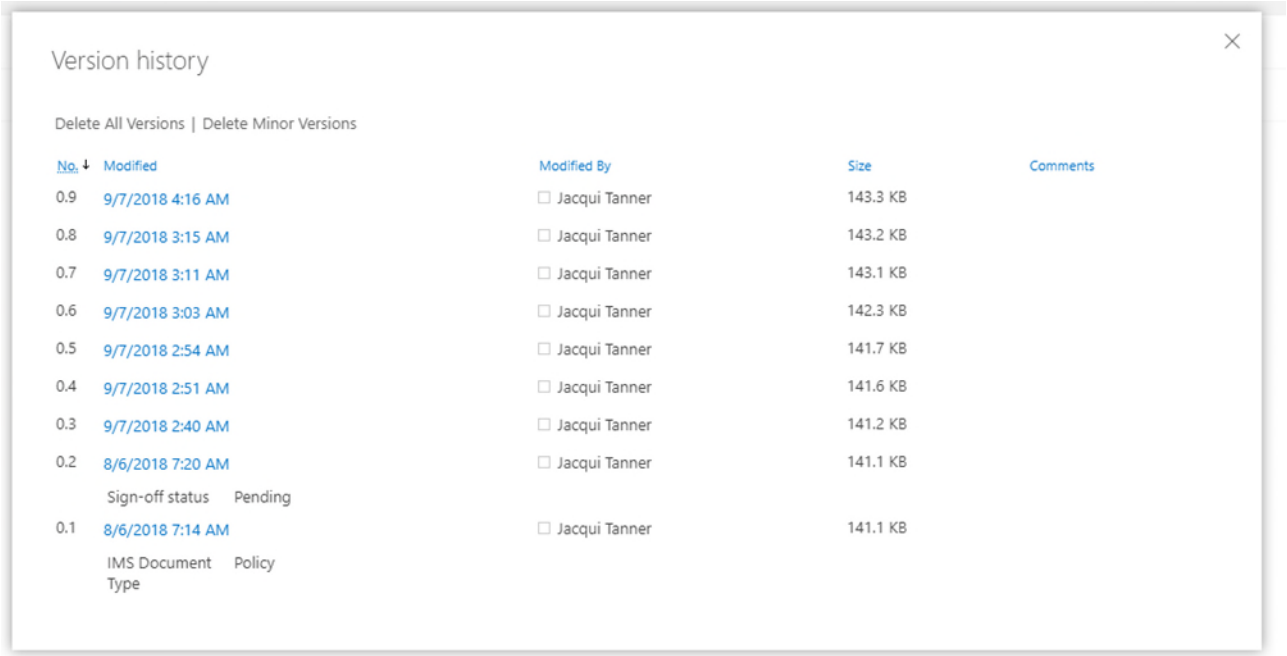


Figure 1 Example document version history in SharePoint

Retrievability

1.31 The DMS is resilient, cloud based and is designed to be always available therefore documents can be retrieved when required. The SharePoint-based DMS allows for document retrieval and has a full audit trail of document access.

Security controls and protection of all Documents

1.32 The Concessionaire and TTL shall work together to identify those Documents which shall be security classified in accordance with Government Security Classifications and apply the appropriate process as specified in the Security Management Plan.

1.33 The Concessionaire has mapped its security classifications to TTL and Government Security Classifications to ensure documents and records are marked with the correct classification. Refer to Table 1.

1.34 SharePoint enables controlled publication and sharing of Documents to relevant parties. The Concessionaire protective marking scheme is part of its ISO27001 framework and documented. This aligns with Government Security Classifications. Information security is managed using a systematic and comprehensive Information Security Management System (ISMS) that is certified against ISO/IEC27001:2013. The Concessionaire's security controls include the Concessionaire operating a clear desk policy. Documents stored in SharePoint will be protected by inbuilt permissions management, built by a SharePoint administrator. Documents will contain the appropriate level of access protection and will inherit permissions based on storage location.

(a) Access levels include:
(b) View/Read only
(c) Contribution
(d) Design
(e) Document Approval
(f) Administration
(g) Vital data back-up will be affected in accordance with our current IT back up procedures.

Table 1 Concessionaire Security classification mapped to TfL and Government Policy

Government Security Classifications	TfL Standard: Information Security Classification	Concessionaire Information Security Classification
OFFICIAL	TfL UNCLASSIFIED	PUBLIC
	TfL RESTRICTED (all information other than personal data)	PROTECTED (default)
	TfL RESTRICTED ('personal data')	
SECRET	TfL CONFIDENTIAL	CONFIDENTIAL
		Confidential \ Internal only (Sub-classification)
		Confidential \ Internal & Trusted (Sub-classification)
		Confidential \ Legally Privileged (Sub-classification)
TOP SECRET	Not used	Not used

Standards

1.35 The Concessionaire's Document Management System follows best practice and adheres to recognised standards including ISO 9001 QMS, ISO27001 for information security.

1.36 The Concessionaire will adhere to the TfL Information and Records Management Policy.

1.37 The Concessionaire will comply with the standards in Schedule 2.3 table 6:

Table 2 INFORMATION GOVERNANCE Policies and Standards

Title / Description	Document Reference	Version	Category
Privacy and Data Protection Policy	P023	A2	Bespoke Standard
Information and Records Management Policy	P114	Issue 2010	Bespoke Standard
Information Access Policy	P113	Issue 2010	Bespoke Standard
Government Security Classifications Policy (May 2018)	None assigned	1.1	Industry Standard
Information Security Policy	None assigned	Issue 2009	Bespoke Standard

1.38 The Concessionaire has several related Group policies which the Concessionaire follows, as listed in the table below. These polices align with the TTL bespoke standards of:

(a) Privacy and Data Protection Policy
(b) Information Access Policy
(c) Information Security Policy

Table 3 Concessionaire Group Information Security and Privacy policies

Information security policies	Privacy policies
Policy Statement	Privacy Policy
Group Data Protection Policy	Intra-Group Processing Agreement
Information Security Policy	Data Protection Impact Assessment
Information Security Classification	Subject Access Request Procedure
Information Security Incident Response	Subject Access Request Form
Standard for Network Security	Personal Information Register
Standard for Secure Software Development	
Standard for Information Handling and Transfer	
Standard for the use of Cryptography	
Standard for User and System Authentication	
Standard for Backup and Archive Security	
Acceptable Use of Information Technology	
Information Security and Projects	
Supplier Security Management	
Security and System Selection	
Document and Personal Data Retention and Disposal Policy	

The draft UK Document and Personal Data Retention and Disposal Policy is ANNEX 2B - UK Document and Personal Data Retention and Disposal Policy.

2 Document Management System

Document management strategy

2.1 The Concessionaire will comply with the requirement set out in Paragraph 2.4, gaining written agreement from TTL where required.

Liaising with TTL in relation to Documents

2.2 The Concessionaire will discuss document management with TTL in order to understanding TTL's requirements. The Concessionaire will then provide a Document Management System that meets all the operational and security requirements to deliver and then manage the Agreement.

2.3 Document management is an essential component of this Agreement, providing a foundation for TTL to work together with the Concessionaire and our Key Sub-contractor Installation Technology, sharing Documents and storing records to deliver the Services.

Sharing

2.4 The Document Management System will comply with the requirement set out in Paragraph 2.8 to enable the controlled electronic management of working Documents between the Parties. This is

explained in more detail in the procedures. Document Security and storage are explained further elsewhere in this Plan.

Software used to generate and manage Documents

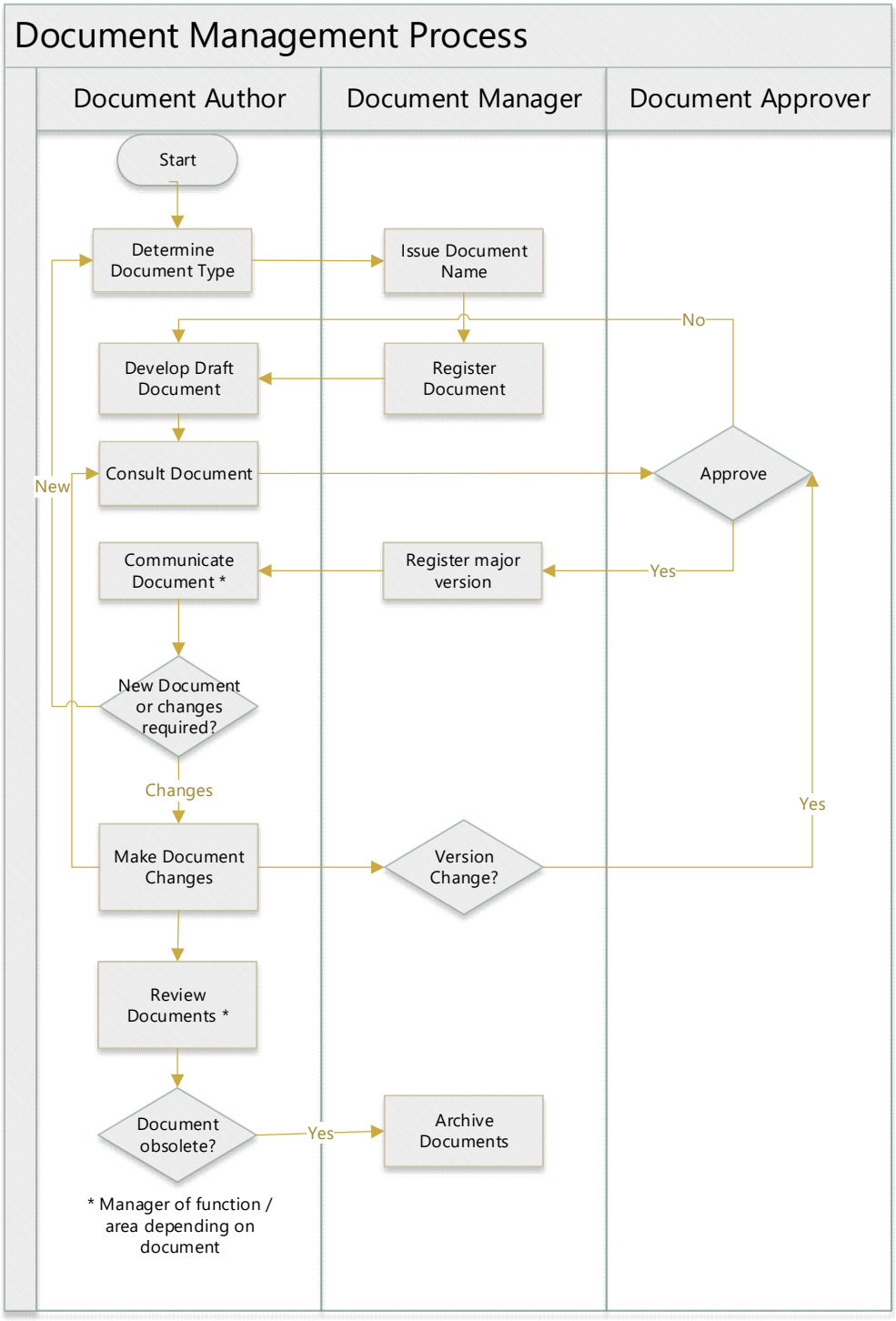
2.5 Microsoft Office 365 (including SharePoint online) is the Document Management System software. Documents may be in any standard application.

2.6 Station and tunnel design drawings are in in CAD. Other technical drawings such as network designs & diagrams may be in Visio.

2.7 Most information systems will have data stores, most applications will generate data and in some cases files that will be held in the DMS. All Documents will be in a format agreed with TTL to meet its requirements.

Document change process

2.8 The Concessionaire Document Management Process below shows the steps to issue a new, or change, a Document. The Concessionaire will look to optimise this process and automate steps where this adds benefit. The step to 'Communicate Document' will be the input to the Document submissions procedure for all documents requiring TTL Approval or Assurance.


Document Management Process
Document Author
Document Manager
Document Approver
Start
Determine Document Type
Issue Document Name
No
Develop Draft Document
Register Document
Consult Document
Approve
New
Communicate Document *
Register major version
Yes
New Document or changes required?
Changes
Yes
Make Document Changes
Version Change?
Review Documents *
Document obsolete?
Yes
Archive Documents
* Manager of function / area depending on document

The table below shows the document change types from major or significant to minor corrections and the level of control and consultation for each type. The change control will ensure that each Document clearly states which other Documents it supersedes.

Table 4 Document change types and level of consultation required

Change Type	Use / Definition	Consultation	Communication	Version Change
Major Change	Fundamental or significant changes to process, accountability or performance standards; Changes that are sufficiently great or important that require the endorsement by the Executive level; Changes that have a significant impact on business resources; Changes that have a significant impact on cross-business interactions;	Director of relevant area for authorisation Management Committee consulted PPM Project Governance	Business-wide or relevant stakeholders	Yes
Moderate Change	Changes to process, accountability or performance standards that are not major in nature Changes to HSE internal standards (i.e. Not regulatory driven); Changes to forms or templates; Changes to full document format.	Director of relevant area for authorisation. Management Committee not routinely consulted PPM Project Governance	Relevant stakeholders	Yes
Minor Change	Editorial changes or corrections to readability, spelling, in-document format, links; Correction of position titles.	Nil	Case by case basis	No

Document retention schedule

2.9 The Concessionaire will provide a document retention schedule setting out which Documents will be retained and for how long in accordance with the provisions of Clause 13 (Records, Reports and Audits).

Document Management System

2.10 The Document Management System conforms to Good Industry Practice. It forms part of the Concessionaire's quality management system and its ISO 9001 standard. The Concessionaire will provide details of the functionality, operation and use of such system to TTL upon request.

Table 5 User Roles Responsibilities and permission

Role	Responsibilities
Concessionaire employees	• Ensure official Documents which need sharing are routinely captured • Ensure access to Documents is managed according to authorised access • Ensure Documents are protected from unauthorised alteration or deletion • Ensure Documents are version controlled as required • Ensure staff time is not lost searching for files • Ensure the Documents are distributed and accessed by authorised staff; and • Ensure records are kept and are clearly identifiable and easily retrievable.
Concessionaire Business Unit managers e.g. Head of Engineering, Head of Operations, PMO Manager	• Ensure that the policy standard and guidelines are documented, approved and followed within the business units for all the Documents stored in the DMS • Provide their business units with assistance in the overall management of Documents stored in the DMS • Clean up their business unit's document repository regularly to remove unwanted and unnecessary Documents • Develop document approval and authorisation process for approval by their Director • Ensure the document approval process is followed within the business unit • Help their business unit with the implementation and interpretation of the Document Management Procedures and Guidelines • Develop, document and obtain sign-off for specific requirements of retention and disposal of Documents as applicable to respective business units • Develop and provide training in document management processes and the DMS • Ensure that the naming convention for the business unit is developed, approved and followed by all the business users within the unit • Develop the appropriate metadata and taxonomy for each Document so that the Document can be searched across all the

Role	Responsibilities
	business units; and • Ensure records are kept and are clearly identifiable and easily retrievable.
Document Manager / controller for TTL within the PMO, dedicated role for deployment phase.	• Manage document security. Documents will be maintained in TTL's SharePoint site for the delivery. This area will only be accessible by the TTL delivery team (including authorised supply chain personnel) including the TTL project sponsor. • Manage document control across organisational boundaries, a suitable common repository (in SharePoint) will be identified in conjunction with TTL and supply chain partners • Manage the development and release of documents such as processes, templates and other project-related documentation. • Management and internal controls for Documents • Own the document register • Manage Document change approvals by a responsible party
TTL Project Manager	• Be responsible for the safekeeping of all the mandatory Documents produced by the project teams.
TTL	• Approve and Assure Documents in line with the Document Submissions Procedure • Access to TTL documents provided by the Concessionaire is only given to approved personnel • Ensure the Concessionaire is informed of any user changes

Audits

2.11 Records, reports and Audits will be shared on request with TTL (as required in Clause 13).

2.12 Sub-contractors will comply with the agreed relevant policies for document and records.

2.13 Audit plans and the audit records are included in the Concessionaire's QMS ISO9001 framework. The Concessionaire's framework includes an internal audit at least once in every 3 years if a process is linked to a high or extreme corporate risk. Where documentation becomes obsolete or redundant, obsolete versions will to be archived and retained for auditing purposes as per the Concessionaire's Company Retention Policy.

Logs and access management

2.14 The Concessionaire's Office 365 retention policies will ensure documents under direct Concessionaire controls are appropriately retained. The Concessionaire will use eDiscovery functionality in Office 365 to respond to TTL requests for access to specific content. Sub-contractors will use the Concessionaire's SharePoint online environments for document storage, or comply with the Concessionaire's document management requirements.

3 Procedures for Managing Documents

Document control

3.1 The Concessionaire will comply with the requirement set out in Paragraph 2.7 to manage document versions to clearly identify the most current version within the Document Management System. This is shown in the Traceability paragraph earlier.

3.2 In respect of any Documents that require Approval by TTL, the Concessionaire shall ensure that the Document Management System captures and records all necessary metadata to verify that the Documents have been Approved by suitably authorised TTL Personnel.

Document sharing and review

3.3 The Document Management System shall meet the requirements set out in Paragraph 2.9.

3.4 The CMDB shall meet the requirements set out in Paragraphs 2.92.9(b), 2.92.9(f), 2.92.9(g)(i) and 2.92.9(j).

Document security

3.5 The Concessionaire's general approach to security is to procure only solutions that are compliant with its information security requirements e.g. data encryption, and have demonstrated commitment to security including the use of Microsoft Azure technologies for identity and security management.

3.6 The Concessionaire will comply with the requirement set out in Paragraph 2.10 to comply with the provisions of Schedule 2.4 (Security Management).

3.7 The Document Management System (and its CMDB system) will be encrypted. OneDrive for Business and SharePoint Online and the CMDB tool ServiceNow, encrypt ‘data at rest’ and ‘data in motion’.

3.8 No data (including all back-ups of such data) will be hosted, stored or transmitted in or to Restricted Countries without the prior consent of TTL.

3.9 User access is maintained on the principle of 'least privilege' so that users of the Document Management System shall only be able to access the information that is deemed necessary for their particular purpose. The details of how that principle is applied is described in the Security controls section above.

3.10 TTL and third party access to the Document Management System will be restricted to devices on TTL-approved public IP addresses. The Concessionaire will create a specific SharePoint site collection and apply the TTL restrictions to that site.

3.11 The Concessionaire will comply with test requirements set out in Paragraphs 2.12 and 2.13

4 Document Register

4.1 The Concessionaire will comply with the requirements set out in Paragraphs 2.15(a) to 2.15(i) and 2.16 to maintain (on a Near Real Time basis) an accurate Document Register and retain details of superseded Documents. When viewing the version history of a Document in SharePoint, any previous version can be opened with a full audit trail of who has edited any version.

Review and Updating

4.2 The Concessionaire will comply with the requirements set out in Paragraphs 2.17, 2.18(a), 2.18(b), 2.19, 2.20, 2.21.

4.3 The Concessionaire will review and, if necessary, update the Document Management Plan on each anniversary of the Effective Date during the Term or more frequently as required.

4.4 New systems or software will be managed using the Concessionaire’s ITIL Release and Change Management process.

4.5 All Designs will be updated throughout the Term to reflect changes to the Telecommunications Infrastructure and As-Built Records within thirty (30) Working Days of such changes or later if agreed in advance at TTL's discretion.

Documents

4.6 The Concessionaire will comply with requirements set out in Paragraphs 3.1(a) to 3.1(h), 3.2, 3.3, 3.4, 3.5 and 3.6.

4.7 Access to the CMDB will be via a different toolset / OSS system and read only access will be provided to TTL's nominated users.

4.8 Wherever possible sensitive security information such as usernames or login details will not be held in traditional documents and will not be shared.

5 Submissions Procedure

Overview

5.1 The Document Submissions Procedure has been summarised in the flow diagram Figure 2.

5.2 The process describes how Documents will be Approved or Assured by TTL as required under this Agreement and the Document Register accurately records each Document.

Approval and Assurance

5.3 The Concessionaire will comply with requirements of the Approval Submissions Procedure set out in Paragraphs 4.4(a), 4.4(b), 4.4(c) and 4.5.

Submission and Iteration of a Document

5.4 Submission and Iteration process is broken down into phases listed in requirement set out in Paragraph 4.8.

Preparation phase

5.5 The Concessionaire will meet the requirement set out in Paragraph 4.9.

Submission and Document iteration

5.6 The Concessionaire will meet the requirement set out in Paragraphs 4.10, 4.11, 4.12, 4.13, 4.14 and 4.15.

Review Period

5.7 The Concessionaire will meet the requirements set out in Paragraphs 4.16, 4.17 and 4.18.

Response Period

5.8 The Concessionaire will meet the requirements set out in Paragraphs 4.19, 4.20, 4.21, 4.22.

Revision Period

5.9 The Concessionaire will meet the requirements set out in Paragraphs 4.23, 4.24, 4.25, 4.26 and 4.27.

Deemed Assurance

5.10 The Concessionaire will meet the requirement set out in Paragraph 4.28.

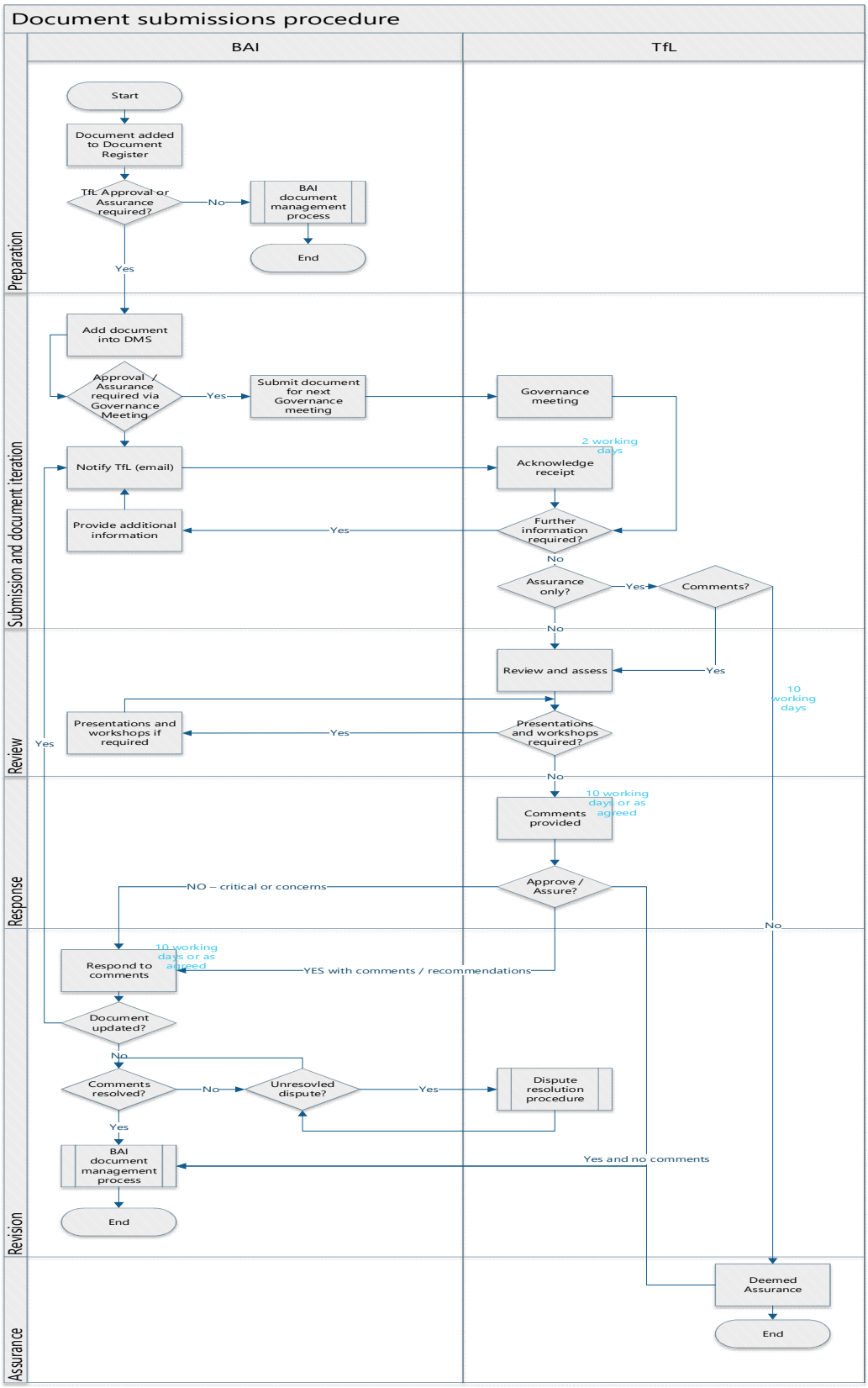


Figure 2 Submissions procedure

ANNEX 2A - Document Management File Plan

Document Template Number	Section / Document title	Security Level	Review Schedule (Yrs after project end)	Disposal Schedule (Yrs after project end)
01.00 Correspondence & Meetings				
	01.01 Incoming Correspondence			
	e-Mails (Incoming)	Protected	7	10
	Fax (Incoming)	Protected	7	10
	Letters (Incoming)	Protected	7	10
	Memos (Incoming)	Protected	7	10
	Transmittals (Incoming)	Protected	7	10
	01.02 Outgoing & internal Correspondence			
	e-Mails (Outgoing/Internal)	Protected	7	10
	Fax (Outgoing/Internal)	Protected	7	10
	Letters (Outgoing/Internal)	Protected	7	10
	Memos (Outgoing/Internal)	Protected	7	10
	Transmittals (Outgoing/Internal)	Protected	7	10
	01.03 Confidential Correspondence (Only use if secure)			
	e-Mails (Confidential/Restricted)	Confidential	7	10
	Fax (Confidential/Restricted)	Confidential	7	10
	Letters (Confidential/Restricted)	Confidential	7	10
	Memos (Confidential/Restricted)	Confidential	7	10
	Transmittals (Confidential/Restricted)	Confidential	7	10
	01.04 Meetings & Schedules			
	Meeting Agendas	Protected	7	10
	Meeting Minutes	Protected	7	10
	Meeting Schedules	Protected	7	10
02.00 Management				
	02.01 Planning			

	Access Plan	Protected	7	10
	Integrated Assurance Plan, Gates Strategy and Gates Plan	Protected	7	10
pd0214	Execution Plan (multiple)	Protected	7	10
	├ Project Governance Process (Schedule 2.1 deliverable) (part of Execution Plan)	Protected	7	10
	Implementation Schedule	Protected	7	10
	Resource Management Plan	Protected	7	10
	├ Mobile Services Outline Implementation Plan (schedule 6.1 Annex 1)	Protected	7	10
	├ Outline Fibre Services Outline Implementation Plan (schedule 6.1 Annex 2)	Protected	7	10
	├ Streetscape Services Outline Implementation Plan (schedule 6.1 Annex 3)	Protected	7	10
	├ Public Wi-Fi Services Outline Implementation Plan (schedule 6.1 Annex 4)	Protected	7	10
	Schedule Baseline Approval	Protected	7	10
PD0218	Progress Reporting Plan	Protected	7	10
PD-10815	Design Management Plan (for DAS only for Bid)	Protected	7	10
T SEMP	Systems Engineering Management Plan (SEMP)	Protected	7	10
PD-10652	├ Human Factors Integration Plan (HFIP)	Protected	7	10
PD-10670	├ Reliability, Availability & Maintainability (RAM) Plan	Protected	7	10
PD-10676	├ Reliability Availability & Maintainability (RAM) Status Report	Protected	7	10
PD-10682	├ Interface Management Plan	Protected	7	10
PD-10674	├ EMC Control Plan	Protected	7	10
PD-10743 Inspection & Testing Strategy Plan / PD0168 / F1076 (IM template)	T&D Project Test Strategy	Protected	7	10
	Service Management Plan	Protected	7	10
	T&D Cut-over Plan	Protected	7	10

	draft detailed Security Management Plan (schedule 2.4. Annex 1 deliverable)	Protected	7	10
	02.02 Governance & Cost			
	Characterisation	Protected	7	10
n (Link in PD doc)	Gate Certificate	Protected	7	10
	Authority Submission	Protected	7	10
	Business Case	Protected *	7	10
PD Estimate	├ Estimate	Protected	7	10
	02.03 Reporting			
PD0218 (Plan)	Progress Report	Protected	7	10
	02.04 Risk, Issues & Value Management			
T Prog RMS / T Proj RMS / PD0045	├ Risk Management Strategy (RMS) (links to Execution Plan)	Protected	7	10
	Risk Register (RAID) (Schedule 2.1 Strategic Risk and Issues Register)	Protected	7	10
PD0217	├ Issue Register	Protected	7	10
	Risk Management Process - part of Project Management Methodology (Schedule 2.1 deliverable)	Protected	7	10
	02.05 Change Control			
PD Change Control Register	Change Control Register	Protected	7	10
	Change Request Form (CRF) (template - will build online and link)	Protected	7	10
	02.06 Resource Management			
	People Change Plan	Protected	7	10
	Organisation Charts (Appendix H of Execution Plan)	Protected	7	10
	02.07 3rd Party & Stakeholder Management			
	├ Benefits and Value (Part of Execution Plan, appendix)	Protected	7	10
PD0222	├ Stakeholder Engagement Plan (Part of Execution Plan, appendix)	Protected	7	10
PD Communications Plan	├ Communications Plan (Part of Execution Plan, appendix)	Protected	7	10

	├ External Consultation Plan (Part of Execution Plan, appendix)	Protected	7	10
	Supplier Quality Assurance	Protected	7	10
03.00 Feasibility & Scope				
	03.01 Brief			
	03.02 Data Capture			
	03.03 Optioneering			
	03.04 Recommendations			
	03.05 Requirements			
PD-10806	├ Verification & Validation Report (SEMP Annex)	Protected	7	10
PD0044/F0859	Project Requirements	Protected	7	10
	Project Requirements Matrix	Protected	7	10
	Scope Definition Reviews	Protected	7	10
04.00 Contracts & Commercial Management (note - from CA/approval these docs move to the relevant folder i.e. Outline in Tender to)				
	04.01 Procurement Strategy			
	Procurement Schedule	Protected	7	10
	Procurement Strategy (AKA Supply Chain Management Plan)	Protected	7	10
	04.02 Quotations & Contractor Estimates			
	RFI responses	Protected		
	RFP responses	Protected		
	04.03 Pre-Qualification Submissions			
	Pre-Qualification Documents (supplier responses)	Protected	7	10
	04.04 Tender Documentation (ITPD)			
	BAI_TCP_ITPD_RESPONSE SCHEDULE 4.1 Concessionaire solution	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 4.2 Commercially Sensitive Information (table)	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 6.1 - Implementation Plans Annex 1-8	Protected		

	BAI_TCP_ITPD_RESPONSE SCHEDULE 6.2 - Outline Test Strategy	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 6.2 - Annex 4 Works Funded by Grants Assurance Process	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 6.2 - Outline Verification Activity Plan	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 8.1 GOVERNANCE	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 8.4 Document Management Plan	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 8.5 Exit Management	Protected		
	4.05 Invitation to Submit Final Tender Documentation (ISFT)			
	Contract Management Plan	Protected	7	10
	Schedule 2.2 Performance Levels (KPIs)	Protected		
	BAI_TCP_ITPD_RESPONSE SCHEDULE 4.5 Business Plan	Protected		
	04.06 Negotiation / Contract Award			
	Schedule 4.5 Business Plan	Confidential		
	Contract Documents	Confidential	7	10
05.00 Design				
	05.01 Design Reviews			
	Benefits Realisation Review (Part of Programme or Project Evaluation Reviews)	Protected	7	10
	Design Reviews	Protected		
	05.02 Design Surveys			
PD-10721	Site Survey	Protected	7	10
	05.03 Design Drawings			
	Design Drawings	Protected	7	10
	Drawing Register	Protected	7	10
	05.04 Design Specifications / Design Pack finals ADAS			
F0879	Technical Requirements Specification (TRS)	Protected	7	10

	Conceptual Design Statement (CDS)	Protected	7	10
	Product Specification	Protected	7	10
	T&D High Level Design Complete list of design docs TBC	Protected	7	10
	T&D Infrastructure Low Level Design	Protected	7	10
	T&D Network Low Level Design	Protected	7	10
	T&D Service Requirements (T&DSR)	Protected	7	10
	T&D Service Model (T&DSM)	Protected	7	10
	T&D Project Warranty Plan	Protected	7	10
	05.05 Design Plans & Reports			
	Interface Definition Document (IDD)	Protected	7	10
	Project Test Plan	Protected	7	10
	Test Plan Template (see Schedule 6.2 annex 3 x12 Milestone test plans linked to 6.1 Milestones)	Protected	7	10
	05.06 Technical Assurance			
PD-10667 f-10667	Configuration Management Plan	Protected	7	10
	Design Check Certificates (S1538)	Protected	7	10
	05.07 Concessions / Non-Compliance			
	05.08 Others Documents (Design)			
	Product lifecycle management Process (schedule 2.1 deliverable)	Protected	7	10
	05.09 Design Specifications / Design Pack finals STREETSCAPE			
	Product Specification	Protected	7	10
	High Level Design	Protected	7	10
	├ Planning approval	Protected	7	10
	├ Drawings	Protected	7	10
	Low Level Design	Protected	7	10
	├ Construction drawings	Protected	7	10
	Legal Agreements	Protected	7	10
	Handover Pack	Protected	7	10
	├ As Built Drawings	Protected	7	10

	├ Commission and test report	Protected	7	10
	├ Photos	Protected	7	10
	├ Configuration Data	Protected	7	10
06.00 Delivery				
	06.01 Access, Logistics & Protection		7	10
	06.02 Forms & Reporting			
	06.03 Permits, Approvals, Certificates & Licences (Consents)			
in folder but no content	Consents Strategy & Plan		7	10
	06.04 Method Statements (Safe System of Work Plan)			
	Method Statement Briefings - Signatures of Acceptance (held by Contractor / Principal Contractor)	Protected	7	10
	Method Statement Register (held by Contractor / Principal Contractor)	Protected	7	10
	06.05 Site Diaries			
	Site Log/Reports (held by Contractor / Principal Contractor)	Protected	7	10
	06.06 Delivery Planning			
	Shift Plan (Day & Night) (held by Principal Contractor)	Protected	7	10
	06.07 Site Management & Site Control			
	Housekeeping Check List (held by Contractor / Principal Contractor)	Protected	7	10
	Site Attendance Registers (held by Contractor / Principal Contractor)	Protected	7	10
	Site Rules - Specific & Generic (held by Contractor / Principal Contractor)	Protected	7	10
	06.08 Other Documents (Delivery)			
07.00 Operations & Commissioning				
	07.01 Tests, Inspections Certificates & Reports			
PD-10747 F0882	├ Verification & Validation Plan (part of SEMP)	Protected	7	10
F0908	EMC Test Specification / Plan	Protected	7	10
F1075 (IM template)	T&D Test Complete Report	Protected	7	10

	Test Issue Management Process (Schedule 6.2 deliverable)	Protected	7	10
	Works Funded by Grants Services Assurance Process (Schedule 6.2 Annex 4)	Protected	7	10
	Test Certificate (Schedule 6.2 Annex 5)	Protected	7	10
	Milestone Achievement Certificate	Protected	7	10
	07.02 Defects			
	Snagging / Defects Register	Protected	7	10
	07.03 Incidents & Failures			
	Incidents & Failures Documents (early-life support / warranty period) In System tbc	Protected *	7	10
	07.04 O&M Manuals			
	Operations Manual	Protected	7	10
	07.05 Red Line & As Built Drawings (final versions) (list TBC)			
	As Built Drawings & Plans	Protected	7	10
	Red Line Drawings & Plans	Protected	7	10
	07.06 Training			
	Completed Training Forms	Protected	7	10
	Training Matrix	Protected	7	10
	07.07 Other Documents (Operations & Commissioning)			
PD-10583 (plan)	Obsolescence Management File	Protected	7	10
	Configuration Management Database (CMDB)	Protected	7	10
	Infrastructure Register	Protected	7	10
08.00 Media Library				
	08.01 Images			
	08.02 Audio & Video			
	08.03 Presentations			
	Presentations	Protected	7	10
09.00 HSEQ				
	09.01 CDM			
	F10 Notification (CDM)	Protected	7	10

	Team HSE Competency Assessment	Protected	7	10
	Health, Safety and Environment Pre-construction Information	Protected	7	10
	09.02 Health & Safety Plans / Hazard Control			
	Asbestos Register (not Risk Assessment	Protected	7	10
	COSHH Check List (no requirement for this)	Protected	7	10
	Engineering Safety Management Plan (Engineering Document under Ian Hewitt)	Protected	7	10
	Construction Management Plan (CMP)	Protected	7	10
	Crime and Disorder Assessment Rationale	Protected	7	10
PD0255	Construction Phase and Environmental Management Plan	Protected	7	10
F0864	Site Emergency Preparedness Plan	Protected	7	10
F0862	Safe System of Work	Protected	7	10
	Fire Safety Strategy	Protected	7	10
	Engineering Safety & Assurance Case (ESAC)	Protected	7	10
	09.03 H&S File			
	Health & Safety File Information	Protected	7	10
	EMC Technical File	Protected	7	10
	09.04 H&S Reports			
	Accident / Incident Reporting Procedure	Protected	7	10
	Environmental Incident Records (held on SHIELD)	Protected	7	10
	Incident Reports (Includes RIDDOR CIRAS & CIRF Forms) (held on SHIELD)	Protected *	7	10
	Work Instructions Document (Planning, Build & Test) based on WI 200		7	10
	09.05 Compliance, Audit & Inspection			
	Audit & Surveillance Plan (outline plan provide in Bid response E)	Protected	7	10

	Site Inspections (outline plan provide in Bid response E)	Protected	7	10
	Sustainability Assessment	Protected	7	10
	Ecology Check	Protected	7	10
F5903	Verification Activity Plan (VAP) (schedule 6.2, Annex 1 Outline VAP)	Protected	7	10
	Congestion, Control & Emergency Plan (CCEP) Update & Engineering Plan	Protected	7	10
	B224 Fire Compliance Submission (template but not in Pathway)	Protected	7	10
	├ LFEPA Exemption (is this part of B224?)	Protected	7	10
	├ Fire Safety Compliance Inspection Report (is this part of B224?)	Protected	7	10
	├ LU FCT Authority To Use Notice (is this part of B224?)	Protected	7	10
	ISO 27001 certificate (Security)	Protected	7	10
	ISO 9001 certificate (Quality)	Protected	7	10
	ISO 14001 certificate (Environment)	Protected	7	10
	ISO18001 certificate (OHS)	Protected	7	10
	ISO 44001 certification plan	Protected	7	10
	GRT1(b) ISO20001 accreditation plan (Schedule 2.1 deliverable)	Protected	7	10
	GRT6(b) ISO55001 accreditation plan (Schedule 2.1 deliverable)	Protected	7	10
	Asset and Infrastructure Management lifecycle process compliant with ISO 55001 (Schedule 2.1 deliverable)	Protected	7	10
	Home and Mobile Working Policy (Schedule 2.4 deliverable)	Protected	7	10
	09.06 Registers, Forms, Reports & Notifications			
	Hazard Log (this is the HSE risk register - top 5 hazards are detailed in bid response E)	Protected	7	10
	Concessions Request	Protected	7	10
	Engineering Safety Hazard Log	Protected	7	10
	09.07 QUENSH			
	QUENSH	Protected	7	10

	09.08 Environment, Quality & Monitoring			
	Environmental Evaluation	Protected	7	10
	Site Noise and Vibration Evaluation and Control	Protected	7	10
	Waste Management Plan (WMP)	Protected	7	10
	Carbon and Energy Efficiency Plan	Protected	7	10
	09.09 Works Plant & Equipment (WPE)			
10.00 Legal Obligations				
	10.01 Statutory Notices			
	10.02 Licences & Approvals			
	Licences & Approvals (Legal Obligations)	Protected	7	10
	10.03 Other Documents (Legal Obligations)			
	Insurance Certificates	Protected	7	10
	Warranties	Protected	7	10
11.00 Handover & Acceptance				
	11.01 Handover & Acceptance			
	Fixed Asset Register (part of CMDB)	Protected	7	10
	Project Completion & Handover Certificate / Delivery Into Service (DIS)	Protected	7	10
	11.02 Completion Review			
	Staged Completion Report		7	10
	11.03 Lessons Learnt			
PD Lessons Learned	Lessons Learned	Protected	7	10
	11.04 Close Out Reporting			
	Financial Close Report	Protected	7	10
	Close Report	Protected	7	10
12.00 Final and Published				
	12.01			
	12.02			
	12.03			
13.00 Human Resources (Optional)				

	Adverts	Protected *	7	10
	Appointment Letters	Confidential *	7	10
	CVs	Confidential *	7	10
	Headcount	Protected *	7	10
	Investors in People	Protected *	7	10
	Job Descriptions	Protected *	7	10
	Personal Information Files (PIs) (Folders & Subfolders by individual or group)	Confidential *	7	10
	Sickness	Confidential *	7	10
	Starters/leavers Forms	Protected *	7	10
	Team Performance	Confidential *	7	10

ANNEX 2B - UK Document and Personal Data Retention and Disposal Policy

DOCUMENT AND PERSONAL DATA RETENTION AND DISPOSAL Policy

Policy Reference	Policy Owner	BAI Companies
	Joel MacMillan	BAI Communications Limited (the Company)

A BACKGROUND

PURPOSE

The purpose of this Policy is to:

a) Promote transparency and accountability, and foster a consistent Document and Personal Data retention and disposal culture across the Company;

b) Ensure compliance with UK Document and Personal Data retention and disposal legislation; and

c) Ensure employee confidence and compliance in their handling, storage and disposal of Documents and Personal Data and being fully informed and aware of their responsibilities and obligations.

STATEMENT

During the course of its activities the Company receives, retains and disposes of Documents and Personal Data from its employees, customers, suppliers and certain other third parties. The correct and lawful treatment of such Documents and Personal Data is key to sustaining the Company's reputation and ensuring we operate successfully. This Document and Personal Data Retention and Disposal Policy sets out the Company's standards and obligations in relation to the retention and disposal of Documents and Personal Data. The Company must only hold Documentation and Personal Data for as long as required and must deploy an effective review mechanism to ensure that this works in practice.

APPROVER

Name	Position	Signature	Date
Billy D'Arcy	CEO		XX August 2019

DEFINITIONS

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller.

"Document(s)/Documentation" means a piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record and includes, but is not limited to:

- Handwritten notes;
- Letters and correspondence;
- Invoices and financial statements;
- Legal contracts;
- Proof of identification and medical information.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Process(es)/Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, enrichment, restriction, erasure or destruction.

"Retention Schedule" means the Schedule(s) that sets out the timeframes that the Company must comply with when retaining and disposing of Documentation and Personal Data, which is set out in Annex 1.

SCOPE

This Policy applies to all departments/individuals who manage the collection, retention and disposal of Documents and Personal Data, including directors, employees and all temporary or contract staff, secondees and consultants whether or not they are employed by the Company and irrespective of length of service or duration of contract.

This Policy sets out how Documents and Personal Data, which are Processed by the Company must be managed through retention and disposal.

This applies to all Documents and Personal Data that the Company possesses, from creation to destruction, inclusive of whether the Documents and Personal Data are printed, written on paper.

RELATED DOCUMENTS

Please also refer to our:

Group Privacy Policy;

Privacy Notices;

Information Security Policy and Statement; and

Group Data Protection Policy

which are located on our Policy Portal Intranet.

RESPONSIBILITIES

Manager, Information Security and Compliance	Provide consultation and support.
Group Company Privacy Officers	Manage compliance with relevant legislation. Provide consultation and support. Review and update Policy as applicable.
Finance Director	Approval and final review of this Policy.

B RETENTION OF DOCUMENTS AND PERSONAL DATA

The Company generally retains Documents and Personal Data as part of its operational needs, and to satisfy legal and regulatory requirements.

Documents and Personal Data must be retained in secure locations in accordance with the Information Security Policy and in the appropriate format to meet their purpose.

The location of Documentation and Personal Data storage must comply with legal and regulatory requirements.

C DISPOSAL OF DOCUMENTS AND PERSONAL DATA

DISPOSAL OF DOCUMENTS AND PERSONAL DATA

The Company generally disposes of operational Documents and Personal Data when they are no longer required to meet the operational needs of the Company or when relevant legislation requires it.

Documents and Personal Data shall be retained in accordance with and for the retention periods set out in the Retention Schedule(s) attached as Annex 1.

Documents and Personal Data, depending on their nature and significance must be disposed of in accordance with our Information Security Policy and related Information Security standards.

THIRD PARTY SHARING OF DOCUMENTATION & PERSONAL DATA

Where the Company shares Documents and Personal Data with third parties, it will ensure that such third parties have adequate procedures for Documents and Personal Data to ensure that the Documents and Personal Data are managed in accordance with our policies, relevant legislation and regulatory guidance. The Company will endeavour to enforce the terms of this Policy through signed contracts with such third parties.

Where the Company is the Data Processor, it will comply with the Data Controller's Document and Personal Data Retention, Storage and Disposal requirements where they are aligned with our contractual, regulatory and legislative obligations.

RECORDS OF DOCUMENT & DATA DISPOSAL & RETENTION

The Company must maintain a formal, written record of its Document and Personal Data disposal and retention processes. Please contact the Compliance manager (reporting to the Finance Director) if you would like to see copies of these records.

While it is the responsibility of the Compliance manager to ensure that this record is accurate and up to date, before undertaking any Document and Personal Data disposal or retention, please review the record to check that your intended disposal or retention fits within the scope of the record and contact the relevant Compliance Manager or your Line Manager before disposing or retaining if you have any doubts.

ACCESS CESSATION ON TERMINATION OF EMPLOYMENT

In case of and with effect as of termination of employment with the Company for whatever reason (termination for cause or without cause, resignation, change of control or divestiture, retirement, etc.), leaving employees must be immediately denied physical and electronic file access, including web-based access and access to cloud applications.

For operational continuity, record preservation needs to be arranged (e.g. by transferring ownership of folders and Documents on Google Drive).

STORAGE OF CONTRACTS IN PAPER OR ELECTRONIC FORM

Contracts may be stored in electronic form only, provided:

a) the contract's integrity can be guaranteed;
b) local law does not require a physical format; and
c) the author can be identified.

These criteria are necessary to preserve the value of the Document in case required as evidence. As a general rule, the greater the value or materiality of a contract, the greater the desirability to retain a paper original. Contracts under seal or requiring notarisation or legalisation need to be retained at least for the relevant retention period in hardcopy form.

LEGAL HOLD

In certain cases, special retention obligations may be imposed ("**Legal Hold**"). Documents relevant to pending or threatened litigation or proceedings, investigations or regulatory inquiries or contracts or agreements that specify that they must be retained for a defined period after the contract or agreement expires shall be excluded from regular document/record destruction and need to be preserved until explicitly otherwise advised by the General Counsel in writing. A suspension may be referred to as "Legal Hold", "Litigation Hold" or "destruction suspension".

TRAINING

The Company will provide all employees with an appropriate level of training relating to Document and Personal Data retention and disposal.

CONTACT DETAILS

The point of contact for enquiries in relation to this Policy should be addressed to Amanda Moore who can be contacted as follows:

BAI Communications Limited

Email: amanda.moore@baicommunications.com.

Address: .4 Kingdom Street, London W2 6BD

BREACH

Breaches of this Policy will be investigated, and appropriate actions taken, which may include termination of employment.

REVIEW

The responsibility for monitoring this Policy rests with the compliance team. This Policy will be reviewed by Simon Lopez or his delegated authority at least on an annual basis.

ANNEX 1 TO ANNEX 2B

RETENTION SCHEDULE

Retention Schedule for BAI Communications Limited

For the different kinds of Documents set out below the following periods for secure storage of data shall apply. The below list is not exhaustive and, for the avoidance of doubt, subject to potential Legal Hold pursuant to Section 14 of the Policy. If you are in doubt as to whether a Document is subject to Legal Hold please check with the General Counsel.

A Company Records (including share registration)

Record Description	Retention Period
Certificate of Incorporation	Life of the Company Best Practice
Certificate of Commencement of Business	Life of the Company Best Practice
Certificate of Company Change of Name	Life of the Company Best Practice
Board Minutes (signed copy)	10 years after date of meeting
Written Resolutions of Board	10 years after date of meeting
Minute Books	Life of the Company Best Practice
Minutes of General and Class Meetings	10 years after date of meeting
Written Resolutions of Members	10 years after date of meeting
Report and Accounts (signed copy)	Life of the Company Best Practice
Interim Reports and Accounts	Life of the Company Best Practice
Circulars to Shareholders (master copy)	12 years
Notices of General and Class Meetings (printed copy)	12 years
Memorandum and Articles of Association (signed original)	Life of the Company Best Practice
Memorandum and Articles of Association (current)	Life of the Company Best Practice
Register of Sealed Documents	Life of the Company Best Practice
Register of Directors and Secretaries (original)	Life of the Company Best Practice
Register of Directors' Interests in Shares and Debentures	Life of the Company Best Practice
Register of Interests in Voting Shares	Life of the Company Best Practice
Register of Charges	Life of the Company Best Practice
Register of Members	Life of the Company Best Practice
Letters of Indemnity for Lost Share Certificates	10 years Best Practice
Trust Deeds Securing Issue of Debentures or Loan Stock (original copy)	12 years
Forms of Share and Debenture Application (originals)	12 years from share issue and permanent microfilmed record
Forms of Acceptance and Transfer	12 years from action date and permanent microfilmed record
Renounced Letters of Acceptance and Allotment	12 years from renunciation and permanent microfilmed record
Renounced Share Certificates	12 years from renunciation and permanent microfilmed record
Share and Stock Transfer Forms	10 years
Requests for Designating or Re-Designating Accounts	12 years after request and permanent microfilmed record
Letters of Request	12 years after request and permanent microfilmed record
Redemption Discharge Forms or Endorsed Certificates	12 years after request and permanent microfilmed record
Signed Forms of Nomination	12 years after request and permanent microfilmed record

Record Description	Retention Period
Stop Notices and other Court Orders	10 years
Directors' Service Contracts	7 years after employment ceases
Registers of Debenture or Loan Stockholders	7 years after stock redemption and permanent microfilmed record
Notification of Change of Address (Shareholders)	3 years
Fully Paid Acceptance and Allotment Letters Exchanged for a Certificate	1 year after ceasing to be valid
Proxy Forms Used at Meetings Convened by Court	1 year after meeting or at direction of Court
Proxy Forms/Polling Cards	1 month after meeting if no poll demanded. 1 year after meeting if poll demanded

B Agreements and Other Related Correspondence

Record Description	Retention Period
All Contracts with Customers and Suppliers	12 years after expiry
Licensing Agreements	12 years after expiry
Rental and Hire Purchase Agreements	12 years after expiry
Indemnities and Guarantees	12 years after expiry
Any Other Contract	12 years after expiry

C Property Records

Record Description	Retention Period
Deeds of Title	Until sold or transferred
Leases	12 years after termination and any terminal queries have been settled
Agreements with Architects or Builders	12 years after completion
Reports and Opinions	12 years after correspondence ends

D Intellectual Property Records

Record Description	Retention Period
Patent and Trademark Records	Life of Company Best Practice
Intellectual Property Agreements and Licences	12 years after expiry
Document Evidencing Assignment of Trademarks	12 years after cessation of registration
Certificates of Registration of Trademarks	12 years after cessation of registration

E Banking Records

Record Description	Retention Period
Instructions to Banks	7 years after ceasing to be effective
Cheques, Bills of Exchange and other negotiable instruments, Invoices, Receipts and Orders for the Payment of Money	7 years after their date of issue
Paying-in Counterfoils	7 years after their date of issue
Bank Statements and Reconciliations	7 years after their date of issue

F Insurance Records

Record Description	Retention Period
Public Liability Policies	Life of the Company Best Practice
Product Liability Policies	Life of the Company Best Practice
Employers' Liability Policies	Life of the Company Best Practice
Other Policies	Until claims under policy are barred
Group Health Policies	12 years after cessation of benefit
Group Personal Accident Policies	12 years after cessation of benefit
Personal Claims	7 years from date of claim
Insurance Schedules	7 years

G Accounting and Tax Records

Record Description	Retention Period
Taxation Returns and Records	10 years
Income and Expenditure	7 years
VAT Records	7 years
Income Tax and NI Returns, including correspondence with Tax Office	3 years after end of Financial Year to which record relates
Budgets and Periodic Internal Financial Reports	2 years

H Employee Records

Record Description	Retention Period
Employee Files	7 years
Senior Executive Records	Life of the Company Best Practice
Redundancy Records	12 years
Personal and Training Records (including disciplinary and grievance hearing notes)	7 years after employment ceases
Payrolls and wage records (including overtime, bonuses and expenses)	7 years
Income Tax Records (eg P45, P60, P58, P48	7 years
Annual Return of Taxable Pay and Tax Paid	7 years
Appointment and Staff Appraisal Records	7 years
Statutory Maternity Pay Records and Calculations	3 years after the end of the tax year in which the maternity period ends
Statutory Sick Pay Records and Calculations	3 years after the end of the tax year to which they relate
Contact Details kept on Personal Files (eg Card Index, MS Outlook	Until it is apparent the person is no longer at the location
Personal Information of any kind on a webpage or website	No longer than the period agreed with the individual

I Health and Safety Records

Record Description	Retention Period
Record of consultations with safety representatives and committees	Life of Company Best Practice
Training records relating to safety at work	Life of Company Best Practice
Risk Assessments for exposure of employees to substances hazardous to health under Control of Substances Hazardous to Health Regulations 2002	40 years from the date of entry of the assessment
Classifications data under Chemicals (Hazard Information and Packaging for Supply) Regulations 1994	3 years after the substance or preparation was supplied

....