SCHEDULE 2.3

SECURITY MANAGEMENT

1. **DEFINITIONS**

In this Schedule, the following definitions shall apply:

"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the Services, Ofwat Premises and/or any Information and Communication Technology ("**ICT**"), information or data (including the Confidential Information and Ofwat Data) used by Ofwat and/or the Delivery Partner and/or any Sub-contractor in connection with this Agreement; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and Ofwat Data), including any copies of such information or data, used by Ofwat and/or the Delivery Partner and/or any Sub-contractor in connection with this Agreement, in either case as more particularly set out in the Security Policy.
"Information Security Assessment"	the assessment provided in response to Appendix C to Ofwat's IT security policy for Delivery Partners.

2. **INTRODUCTION**

2.1 The purpose of this Schedule is to ensure a good organisational approach to security under which the specific requirements of this Agreement will be met.

2.2 This Schedule covers:

2.2.1 the creation and updating of the Information Security Assessment; and

2.2.2 obligations in the event of any actual or attempted Breach of Security.

2.3 Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security.

2.4 The Delivery Partner shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Ofwat Data and/or Confidential Information and any system that could directly or indirectly have an impact on that information, and shall ensure that Ofwat Data and/or Confidential Information remains under the effective control of the Delivery Partner at all times.

2.5 The Delivery Partner shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to Ofwat.

2.6 Ofwat and the Delivery Partner acknowledge that information security risks are shared between the Parties and that a compromise of either the Delivery Partner's or Ofwat's

security provisions represents an unacceptable risk to Ofwat requiring immediate communication and co-operation between the Parties.

2.7 The Delivery Partner acknowledges that Ofwat places great emphasis on the reliability of the performance of the Services, and on the confidentiality, integrity and availability of information and consequently on security.

2.8 References to standards, guidance and policies contained or set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Delivery Partner from time to time.

2.9 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Delivery Partner should notify Ofwat's Representative of such inconsistency immediately upon becoming aware of the same, and Ofwat's Representative shall, as soon as practicable, advise the Delivery Partner which provision the Delivery Partner shall be required to comply with.

3. INFORMATION SECURITY ASSESSMENT

Introduction

3.1 The Delivery Partner's Information Security Assessment shall comply with the requirements of Paragraph 3.2 throughout the Term.

3.2 The Information Security Assessment shall:

3.2.1 comply with the Security Policy;

3.2.2 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Delivery Partner;

3.2.3 detail the process for managing any security risks from Sub-Contractors and third parties authorised by Ofwat relating to the provision of the Services, processes associated with the delivery of the Services, Ofwat Premises and any ICT, Information and data (including Ofwat's Confidential Information and Ofwat Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

3.2.4 unless otherwise specified by Ofwat in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including Ofwat Premises and any ICT, Information and data (including Ofwat's Confidential Information and Ofwat Data) to the extent used by Ofwat or the Delivery Partner in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

3.2.5 set out the security measures to be implemented and maintained by the Delivery Partner in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Delivery Partner complies with the provisions of this Schedule;

3.2.6 at all times provide a level of security which:

(a) is in accordance with the Law and this Agreement;

(b) as a minimum demonstrates Good Industry Practice;

(c) complies with the Security Policy; and

(d) meets any specific security threats of immediate relevance to the Services and/or Ofwat Data and/or Confidential Information;

3.2.7 document the Delivery Partner's security incident management processes and incident response plans;

3.2.8 (where relevant) set out the plans for transitioning all security arrangements and responsibilities from those in place immediate prior to the Effective Date to those incorporated in the Information Security Assessment within the timeframe agreed between the Parties;

3.2.9 meet the relevant standards in ISO/IEC27001 and ISO/IEC27002; and

3.2.10 be written in plain English in language which is readily comprehensible to the Delivery Partner Personnel and Ofwat staff engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

3.3 In the event that the Information Security Assessment is not completed by the Delivery Partner before the Effective Date, the Delivery Partner shall submit the Information Security Assessment to Ofwat within ten (10) Working Days of the Effective Date. If the Information Security Assessment is not approved by Ofwat, the Delivery Partner shall amend it within ten (10) Working Days of a notice of non-approval from Ofwat and re-submit it to Ofwat for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of the first submission to Ofwat of the Information Security Assessment. If Ofwat does not approve the Information Security Assessment following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by Ofwat pursuant to this Paragraph may be unreasonably withheld or delayed. Any failure to approve the Information Security Assessment on the grounds that it does not comply with the requirements set out in Paragraph 3.2 shall be deemed to be reasonable.

3.4 Approval by Ofwat of the Information Security Assessment pursuant to Paragraph 3.3 or of any change or amendment to any information contained within the Information Security Assessment shall not relieve the Delivery Partner of its obligations under this Schedule.

4. BREACH OF SECURITY

4.1 Either Party shall immediately notify the other in accordance with the security incident management process approved as set out in the Information Security Assessment upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

4.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 4.1, the Delivery Partner shall immediately take all reasonable steps (which shall include any action or changes reasonably required by Ofwat) necessary to:

4.2.1 minimise the extent of actual or potential harm caused by any Breach of Security;

4.2.2 remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Ofwat Equipment and/or Ofwat

Data and/or Confidential Information at no cost to Ofwat to the extent that this is within the Delivery Partner's control;

4.2.3 prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure;

4.2.4 supply any requested information or data to Ofwat on Ofwat's request within two (2) Working Days and without charge (where such requests are reasonably related to a Breach of Security or any potential or attempted Breach of Security); and

4.2.5 as soon as reasonably practicable provide to Ofwat full details of the Breach of Security or the potential or attempted Breach of Security, including a root cause analysis where required by Ofwat.

4.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance with the Security Policy or the requirements of this Schedule, then any required change shall be at no cost to Ofwat.

ANNEX 1: SECURITY POLICY

Information Security Policy for third parties

Background

The Water Services Regulation Authority (Ofwat) treats its information as a valuable asset. It is essential that our information must be protected, together with the systems, equipment and processes which support its use. Our information assets may include data, text, drawings, diagrams, images or sounds in electronic, magnetic, optical or tangible media. Our information assets also include personal data for which Ofwat is the Data Controller.

In order to protect Ofwat's information appropriately, third parties must provide security measures and safeguards proportionate to the nature and use of the information. All third parties providing services to Ofwat must comply, and be able to demonstrate compliance, with Ofwat's relevant policies and standards.

All staff working for a contractor and where relevant sub-contractors, with access to Ofwat IT systems, premises or Ofwat information must be made aware of these requirements and must comply with them.

The following are key requirements and all third parties must comply with relevant Ofwat policies concerning:

General

All third parties must implement appropriate arrangements which ensure that Ofwat's information is protected in accordance with prevailing statutory and central government requirements. These arrangements will clearly vary according to the size of the organisation.

It is the third party's responsibility to monitor compliance of any sub-contractors and provide assurance to Ofwat. Sub-contractors can only be contracted with the express permission of Ofwat.

Ofwat undertakes an assessment of information risk for each contract or service that is procured. It grades risk as Low, Medium and High.

Where the assessment of risk is High, Ofwat will require that the third party produce an agreed security plan, to demonstrate the necessary controls when handling, processing or transferring information. An Information Security Assessment template is given in Appendix C.

Ofwat may require further information on completion of the Information Security Assessment to clarify any concerns and provide further assurance regarding the information being processed.

Failure to comply with any of the above or the policies or standards below could result in termination of contract.

Personnel security

Staff vetting should be in accordance with government requirements for pre-employment checks as set out in Appendix A.

Third party staff should be made aware of Ofwat security policies and any specific contract requirements before they begin any works or services.

Protection of information

All third parties handling information that has been protectively marked by Ofwat, in accordance with its Protective Security Markings guidance, must comply with the security measures and standards as determined by the HMG Security Policy Framework (which can be accessed on the Cabinet Office's website at http://www.cabinetoffice.gov.uk/spf.aspx).

The physical and electronic handling, processing and transferring of Ofwat information should be completed using proportionate security measures that include secure access to systems and the use of encryption where appropriate.

All information from May 2018 in government is classified as OFFICIAL whether it is marked or not. Guidance on the changes to Government Security Classifications can be found here. Where information is not explicitly protectively marked by Ofwat we still require controls that are proportionate to the sensitivity of the information whether it be commercially sensitive, legally privileged or public domain information.

We have included in Appendix B the "Guidance for UK Contractors on the Protection of UK Restricted Assets". Whilst this document still refers to the old protective marking scheme descriptors (RESTRICTED) it is still highly relevant to our OFFICIAL-SENSITIVE information assets and should be referenced in that context until the document is formally updated.

Portable and recordable media

Sensitive information that should not be in the public domain, stored on laptops and any recordable media (e.g. CD/USB) should be protected as a minimum by a FIPS 140-2 approved full disk encryption solution.

Protection of personal data

Processing of Ofwat personal and sensitive personal data must at all times comply with the General Data Protection Regulation (GDPR) 2016.

Premises security

The necessary security access controls should be in place at any third party premises where Ofwat information may be held.

Similarly when a third party is working on Ofwat premises they will be subject to our onsite access controls. Further information is requested within the Information Security Assessment.

Security incidents

Third parties must identify, manage and agree reporting procedures for actual or suspected security breaches. In relation to personal data the GDPR stipulate that all breaches of personal data should be mandatorily reported within 72 hours to the Information Commissioner's Office (ICO) as well as the data controller. Data Processors are liable under the GDPR for any breaches of personal data.

Appendix A: Staff Vetting Procedures

The Cabinet Office issued version 4.0 of "Guidance on the pre-employment screening of civil servants, members of the armed forces, temporary staff and government contractors" in May 2018. This was entitled "HMG Baseline Personnel Security Standard (BPSS)" and describes good practice in recruitment checks to address the problems of identity fraud, illegal working and deception generally. The Baseline Personnel Security Standard (BPSS) checks entail identity, nationality and criminal record checks.

Any contractor's staff (including sub-contractor's staff) to be given access to Ofwat's assets (defined as premises, systems, information or data) are subject to the BPSS checks i.e. they are subject to the same checking regime as that for government employees. Unless otherwise stated in the relevant contract, the contractor is required to satisfactorily complete the checks in respect of each individual before they are permitted access to Ofwat's assets. However the Standard need not be applied in those cases where contractor's staff accessing Ofwat's assets are accompanied and supervised by Ofwat personnel at all times.

Ofwat currently holds information classified at OFFICIAL and OFFICIAL-SENSITIVE level. If exceptionally access is required to classified information at SECRET and above then additional **national security vetting** checks will be required.

Appendix B: UK Restricted Security Conditions - Guidance for UK Contractors on the Protection of UK Restricted Assets

Definitions

1. The term "Authority" means the Contracting Authority.

Security Grading

2. The Authority shall issue a RESTRICTED Aspects Letter which shall define the RESTRICTED matter that is furnished, or which is to be developed, under this Contract. The Contractor shall mark all RESTRICTED documents which he or she originates or copies during the Contract with the equivalent national grading.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract have notice that these statutory provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

Protection of RESTRICTED Information

4. RESTRICTED information shall be protected in a manner to promote discretion in order to avoid unauthorised access. The Contractor shall take every effort to prevent the loss or compromise of the information or deliberate or opportunist attack.

5. Disclosure of RESTRICTED information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than a person directly employed by the Contractor or sub-Contractor or Service provider.

6. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or if directed by the Authority, destroyed in accordance with paragraph 23.

7. When not in use RESTRICTED documents shall be stored under lock and key.

Access

8. Access shall be confined to those individuals who have a "need-to-know" and whose access is essential for the purpose of his or her duties.

9. The Contractor shall ensure that all individuals having access to RESTRICTED information meet legal requirements in respect of immigration and the right to work in the UK and have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to RESTRICTED information. Further details and the full requirements of the BPSS can be found at the Cabinet Office website within the Security Policy Framework at Mandatory Requirement 23: http://www.cabinetoffice.gov.uk/spf

Transmission of RESTRICTED Information

10. RESTRICTED documents shall be transmitted, both within and outside company premises in such a way as to make sure that no unauthorised person has access. They may be sent by ordinary post in a single envelope. The word RESTRICTED must **NOT** appear on the envelope. The envelope should bear a company stamp that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

11. Advice on the transmission of RESTRICTED documents abroad or any other general advice including the transmission of RESTRICTED hardware should be sought from the Authority.

Use of Communications and IT Systems

12. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure that they are blocked.

13. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or exfiltrate data.

14. The following describes the minimum Accreditation security requirements for processing and accessing RESTRICTED information on IT systems.

    a. **Access:** Physical access to all hardware elements of the IT system is to be strictly controlled.

b. **Identification and Authentication (ID&A):** All systems shall have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session.

c. **Passwords:** Passwords are part of most ID&A, Security Measures. Passwords shall be minimum of 6 characters long (9 is preferred) and shall include numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

d. **Internal Access Control:** All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. **Data Transmission:** RESTRICTED information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using commercial encryption devices accepted by the Authority. Advice on encryption requirements for the transmission of RESTRICTED information shall be sought from the Authority However, in cases where there is a pressing business need, telephone conversations, video conferencing or facsimile transmissions containing RESTRICTED information may be in clear text. In cases where a pressing business need has been identified, both parties need to accept that there exists the potential for a risk of compromise. When taking a decision to communicate RESTRICTED information in this way they should be aware of the impact of disclosure.

f. **Security Accounting and Audit:** Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

I. All log on attempts whether successful or failed.

II. Log off (including time out where applicable).

III. The creation, deletion or alteration of access rights and privileges.

IV. The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

I. Type of event,

II. User ID,

III. Date & Time

IV. Device ID

The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the

records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

g. **Integrity & Availability:** The following supporting measures shall be implemented:

(1) Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)
(2) Defined Business Contingency Plan
(3) Data backup with local storage
(4) Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).

h. **Logon Banners:** Wherever possible, a "Logon Banner" shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

(1) A suggested format for the text depending on national legal requirements could be:
I. "Unauthorised access to this computer system may constitute a criminal offence"

i. **Unattended Terminals:** Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. **Internet Connections:** Computer systems shall not be connected direct to the Internet unless protected by a firewall which is acceptable to the Authority's Security Officer.

k. **Disposal:** Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Hardware

15. Hardware, such as laptops and Surface Pros holding any information supplied or

generated as a consequence of the contract are to have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed.

16. Unencrypted equipment not on a secure site[1] are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Business Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration.

17. Unencrypted SP3s, laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term "drives" includes all removable recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

18. Any tokens, touch memory devices or password(s) associated with the encryption package are to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

19. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss

20. Any loss of RESTRICTED information shall be reported without delay to the Authority.

Sub-Contracts

21. The Contractor may not Sub-contract any elements of this Contract to Sub-contractors within the United Kingdom without permission of the Authority. When doing so these security conditions shall be incorporated within any Sub-contract document. The prior approval of the Authority mustl be obtained should the Contractor wish to Sub-contract any elements of the Contract to a Sub-contractor in another country.

Publicity Material

22. Contractors wishing to release any publicity material or display hardware that arises from this contract, whether directly or indirectly, must seek the prior approval of the Contracting Authority. Publicity material includes open publication in the contractor's publicity literature or

[1] Secure sites are defined as either Government premises or secured offices on the contractor premises

website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Authority, or any other government department. For Private Venture Defence Related Material to be released at exhibitions, contractors must seek the prior approval of DBRDefSy(S&T/Ind).

Destruction

23. As soon as soon as no longer required RESTRICTED information/material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces.

24. Unwanted RESTRICTED information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation

25. Advice regarding the interpretation of the above requirements should be sought from the Authority.

Audit

26. Where considered necessary by the Authority the Contractor shall permit the inspection of the Contractors processes and facilities to ensure compliance with these requirements.

Appendix C: Information Security Assessment

1. Introduction

Information law requires that whenever Ofwat uses a contractor to process information on its behalf, it must choose a contractor who can offer adequate safeguards to ensure the information is kept safe and secure. Ofwat must also be able to demonstrate it has taken these steps.

2. Purpose of document

This document should be completed by a contractor. It will allow Ofwat to make an assessment of the technical and organisational measures that they have in place to protect the personal information it processes on behalf of Ofwat. It will also act as evidence that Ofwat has taken reasonable measures to ensure these are in place.

It may sometimes be necessary for Ofwat to ask for evidence to support any details supplied on this form and occasionally a site visit may be necessary.

3. Guidance for Contractors.

Ofwat requests that you complete this self- assessment and return it to your contact at Ofwat.

Please do:

- **Raise questions and/or concerns relating to information that you process on behalf of Ofwat and includes the information supplied to you by Ofwat or that you collect or create on its behalf.**
- **Keep evidence and records of compliance with any regulations e.g. Data Protection law.**
- **Ensure that staff understand their responsibilities whether under Data Protection law and/or any obligation of confidentiality.**
- **Review existing contracts with subcontractors to ensure that they meet the strict standards Ofwat is asking of you.**
- **Where the question is not relevant to this contract please state Not Applicable.**

Your business details

Company/organisation name

Number of staff employed	Number of sub-contractors employed

Company address

Ofwat contact details
With regard to the contract in question, specify the name and contact details of your contact at Ofwat

To be completed by the person filling in the form

Name	
Job title	
Telephone number	
Email	
Signature	
Date	

Information overview

Q1	Please provide a detailed description of the work you are carrying out on behalf of Ofwat or for which you are tendering

Q2	Please provide your Data Protection Notification Number. If you are exempt from having to register with the Information Commissioner please explain the reasons why

Q3	Will the information you process on behalf of Ofwat be held at the company address you have given on page 3	Yes/No

Q4	If the answer to Question 3 is NO please provide details of all the addresses where the information will be processed / stored. This includes any Cloud Storage facilities you use, Cloud Storage accreditation, Penetration Testing Evidence and Cloud Security Principles	Yes/No
If YES then please provide the address of the other site(s)		

Q5	Cloud storage: Do you use this type of storage (including as a backup)?	Yes/No
Q5a	If yes, which provider do you use? Where are they located?	
Please provide details		
Q5b	What industry standard(s) has the Cloud Storage Provider got?	

Q6	Please indicate the types of personal/sensitive information you expect to be processing on behalf of Ofwat

Name	☐
Address/post code	☐
Telephone No.	☐
Date of Birth or Age	☐
Gender	☐
Employment status	☐
Dependent Details	☐
Income	☐
Racial/Ethnic origin	☐
Political opinions	☐
Religious or philosophical beliefs	☐
Whether a member of a trade union	☐
Health data	☐
Sexual life or sexual orientation	☐
Criminal convictions & offences	☐
Genetic or biometric data	☐
Others, please specify	

Q7	If collecting personal information from individuals on behalf of Ofwat, do you explain to the individuals the reasons you are gathering the information (e.g. In Privacy Statements, Policies), the exact purposes for which it will be used and any other parties with whom it may be shared?	Yes/No
If YES, please provide details on how you do this		

If you do not collect information on Ofwats behalf please state 'Not applicable'

Q8	With regard to the personal information you process on behalf of Ofwat – do you disclose this information to anyone other than Ofwat?	Yes/No
If the answer is YES, please provide details and reasons for disclosure		

Premises security

IMPORTANT: When completing this section please provide answers that relate to the premises where the information you collect or process on behalf of Ofwat will be stored or processed. If there are more than one premises, please state this and provide answers for each of the premises.

Q9	If you have a reception area, how is it controlled?
Please provide details	

Q10	If there are any other entrances or exits, how are these controlled?
Please provide details	

Q11	Is the office area visible to a casual enquirer at reception or from outside?	Yes/No
Please provide details		

Q12	Do staff wear identification?	Yes/No
If NO please provide details of why		

Q13	Are visitors required to wear identification?	Yes/No
If NO please provide details of why		

Q14	Are there any other measures taken to ensure that access to the premises is restricted to authorised staff and visitors only?	Yes/No
If NO please provide details of why		

Q15	Are there alarm systems protecting the premises?	Yes/No
Q15a	Are these systems linked to the police?	Yes/No
Q15b	Are these systems linked to a monitoring service?	Yes/No

Q16	Are there windows on the premises? (If Yes please answer the questions below)	Yes/No
Q16a	Lockable?	Yes/No
Q16b	Fitted with blinds?	Yes/No
Q16c	Fitted with grids, bars etc.?	Yes/No
Q16d	Covered with security film?	Yes/No
Q16e	Easily accessible from public areas?	Yes/No

Q17	Are the premises where the information is kept, protected by:	Yes/No
Q17a	Security patrols?	Yes/No
Q17b	24-hour CCTV surveillance?	Yes/No

People and policy

Q18	What measures are in place to ensure that all staff are aware of their responsibilities under the requirements of data protection legislation?
Please provide details	

Q19	What steps are taken to ensure the staff you employ are responsible and reliable?
Please provide details	

Q19a	What steps have you taken to ensure your staff have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality?
Please provide details	

Q20	What policies, procedures, training or other measures have you taken to adopt the security standard ISO27001/2?
Please provide details, including why you have not adopted the standard (if applicable)	

Q21	Is there a Data Protection and/or Information Security Policy in place?	Yes/No
Please provide details of which policies you have		
Q21a	Do you have Bring Your Own Device (BYOD) and Working from Home policies? If yes, please provide details.	Yes/No

Please provide details

Q21b	**How do you monitor compliance with these policies?**	Yes/No
Please provide details		

Q21c	**Can it be demonstrated that a breach of the policies is a disciplinary offence within your organisation? If yes, how?**	Yes/No
Please provide details		

Sub-contractors

Sub-contractors cannot be used without the authorisation of Ofwat. If permission is being sought to use sub-contractors it is important to establish what technical and organisational safeguards they have in place.

Q22	**Will you use sub- contractors (or other third party) to process any of Ofwat's information as part of this contract?**	Yes/No

Q23	**How do you ensure that the sub-contractors you use have sufficient technical and organisational safeguards in place to protect the information you give them (i.e. Ofwat's information)?**
Please provide details of the measures you take	

Q24	**Please provide the names and addresses of the companies you will be using as sub-contractors for this contract.**

Other safeguards

These measures should be appropriate to the nature of the information being processed and take into account the harm which would be caused should any unauthorised loss, disclosure or destruction of the information occur.

Restricting access to information

Q25	What measures are in place to restrict staff from accessing information they may not be entitled to on computers?
Please provide details	

Q26	What measures are in place to restrict staff from accessing other types of information e.g. paper records and information held on various media such as DVDs, memory sticks?
Please provide details	

Business continuity

Q27	With regard to information held on computers /servers is it backed up on a daily basis? If yes, please provide details as to where (this includes Cloud facilities)	Yes/No

Q28	Are backup tapes / discs and other media stored off site? If yes, where are they held?	Yes/No
If you have answered NO, are there other precautions taken to protect data against fire/flood and other disasters?		

Q29	What precautions are taken to protect information that is not backed up on computers (e.g. paper file) against fire/flood and other disasters?
Please provide details	

Securely disposing of information

Q30	How do you safely and securely dispose of information held on paper?
Please provide details	

Q31	How do you safely and securely dispose of obsolete hardware and software from which information could be recovered?
Please provide details	
Q31a	**If you use a Cloud storage solution, how do you ensure secure and permanent deletion of information that could be recovered from the Cloud?**
Please provide details	

Encryption technology

Q33	**Depending upon the nature of the contract, the information shared with you may or may not be highly confidential. If Ofwat has classed the information as confidential, it must be delivered to you by secure means and it may also be necessary for it to be sent back by secure means, for example by secure connection (HTTPS). Please describe below the facilities/options you are able to provide for the safe receipt and delivery of confidential information**	Yes/No
Please provide details		

Thank you for taking the time to complete this questionnaire. Please return it to your contact at Ofwat for assessment.

The information you supply will form part of the tendering process and will not be used or shared with other parties. The information you supply will be kept in accordance with Ofwat's retention and disposal schedule.