Physical, Personnel and Cyber Security Requirements for Bidders

This document supports the tender stages of the RTGS Renewal Technology Delivery Partner Procurement Process (**Procurement**). It is relevant for those suppliers that are invited to participate in the Invitation to Participate (**ITP**) stage in the Procurement following completion of the Supplier Qualification (**SQ**) stage (**Bidders**). It is being shared by the Bank now to provide Bidders with an early sight of the requirements which will be in place during the next stages of the process.

It summarises the mandatory physical, personnel and cyber security requirements (**Security Requirements**) that will be required to be followed in regards to the handling of Bank assets and information during the next stages of the Procurement.

1. Scope: The Scope of Security Requirements

1.1 All Bidders should enact the Security Requirements listed herein, in relation to any Bank assets, examples of which are included in paragraph 1.4 (**Bank Assets**).

1.2 Bidders are required to ensure any relevant third parties e.g. sub-contractors and consultants apply these Security Requirements when dealing with Bank Assets.

1.3 From time to time, the Bank may review the implementation of the Security Requirements within any of the Bidders' location(s) in which Bank Assets are, or are intended to be, held or accessed (**Premises**).

1.4 The Security Requirements apply to all Bank Assets. Assets include:

1.4.1 **Information in any form**, which would be categorised as Bank Confidential, Bank Secret or Top Secret as defined in Appendix 1. This includes any information which is printed, written, stored electronically, transmitted by post or electronically, recorded on film, or spoken in conversation. It also includes information regarding access to systems and processes (**Bank Information**).

1.4.2 **Bank property**, including the Bank's technology estate, hardware, objects that are wholly or in part owned or leased by the Bank, and any items the Bank is guarded with protecting (**Bank Property**).

1.5 Cyber security is concerned with ensuring confidentiality (protecting systems, processes and sensitive information so that it is accessible only to those authorised to use it), integrity (safeguarding the accuracy and completeness of information, assets and infrastructure) and availability (ensuring authorised users always have access to information when they need it).

1.6 The Security Requirements apply to all individuals employed or engaged in any way by the Bidder with regard the Bidder's participation in the Procurement. This includes all employees (including those on fixed term contracts), non-executive directors, interns, volunteers, external academics with whom Bank information is shared, contractors and sub-contractors, consultants, agency workers and employees of Bidders involved in the Procurement (together the **Staff**).

1.7 If a Bidder has any doubt as to the applicability of the content of these Security Requirements, they should consult the Bank.

2. Organisation of Information Security

2.1 Bidders must have a named Security Officer for the duration of their participation in the Procurement. This Security Officer must be a member of the Supplier's team assigned to its participation in the Procurement (**Bid Team**). The Security Officer will maintain responsibility for ensuring all staff adhere to these Security Requirements and must raise any concerns regarding the Security Requirements with the Bank.

2.2 The Security Officer should also lead on managing access to Bank Information for the entirety of the Procurement. Such individual must:

2.2.1 confirm that each of the Bidders Staff only have access to Bank Information to perform their roles;
2.2.2 validate the access permissions for each of the Bidder's Staff on a 'need to know' basis;
2.2.3 revoke access to Bank Information where individuals are no longer involved in the Procurement.

2.3 Bidders must follow a documented information security approach (referred to as an ISMS by ISO 27001) covering the Bidder's involvement in the Procurement. The document must:
2.3.1 align with relevant industry-recognised information security standards such as ISO27001 or NIST;
2.3.2 be approved by Bidder senior management; and
2.3.3 be published and communicated to all of the Bidder's Staff.

2.4 Bidders must have a documented incident management process and respond to physical, personnel, or information security incidents relating to Bank Assets, including:
2.4.1 notifying the Bank of any potential loss or compromise of Bank Information as soon as they are aware and no later than 24 hours of an incident;
2.4.2 assisting the Bank as soon as they become aware of a potential incident;
2.4.3 having the capability to collect and provide evidence in a forensically sound manner;
2.4.4 containing and resolving the incident in a timely manner; and
2.4.5 performing post-Incident reviews for all information security incidents related to their participation in the Procurement;

2.5 Where there is any breach of these Security Requirements, Bidders must provide full assistance with any investigation led by the Bank. The Bank reserves the right to remove a Bidder from the Procurement for a breach of the Security Requirements.

3. Personnel Security

3.1 Bidders must ensure that all members of Staff in their Bid Team have UK government security clearance (**SC clearance**) validated by the Bank's Vetting team before accessing any Bank Information.

3.2 Bidders must ensure that members of Staff who are not part of the Bid Team and require access to Bank Information are granted access: (i) on a 'need to know' basis; and (ii) in accordance with the remainder of these Security Requirements.

3.3 Staff who maintain an existing SC clearance will have their clearance reviewed and transferred to the Bank for the duration of their time working on the Procurement. The Bank's Vetting team will manage the transfer of existing SC clearances.

3.4 The Bank's Vetting team may review the Vetting file of any Staff member with existing SC clearance on a case by case basis before approving a transfer.

3.5 SC clearance is restricted to individuals who are resident within the UK and have an address history for the past 5 years. If a Bidder intends to provide access to Bank Information to Staff who are not resident in the UK, this should be flagged as soon as possible to the Bank:

3.5.1 the Bank will seek to undertake security checks on such individuals to provide a level of assurance on each individual equivalent to that provided by SC clearance;

3.5.2 where such assurance can, in the Bank's discretion, be provided, the Bank will allow such individuals access to the relevant Bank Information. Where the Bank cannot gain the necessary assurance, Bidders shall **not** provide that individual with any access to the Bank's Information.

3.6 Bidders must report any personnel or behavioural incidents or concerns in relation to the Staff that they become aware of to the Bank's Security Vetting Team, if that incident is likely to impact on the individual's ability to hold security clearance.

3.7 Where requested Bidders may be asked to provide the Bank with a list of Staff with potential access to Bank Information, software and equipment, along with their access permissions.

3.8 Bidders must define and implement processes for employment termination or change of employment. These processes must include:

3.8.1 notifying the Bank that a Staff member is leaving the Bidder, the Bid Team, or ceasing to be involved in the Procurement, where the that Staff member has access to Bank IT systems or Bank Information;

3.8.2 removing access to Bank Information or Bank IT systems on or before the last day of service;

3.8.3 verifying that Bank owned devices that can store or access Bank Information have been returned on, or before, the last day of service; and

3.8.4 providing the Bank suitable evidence that these processes have been followed.

4. Operations and Physical Security

4.1 Bidders must maintain a secure physical environment at their Premises during the entirety of the Procurement and:

4.1.1 provide layered security zoning within any Premises;

4.1.2 provide audited access controls for physical access to Bank Assets;

4.1.3 detect and alert the Bank to any unauthorised access of Bank Assets.

4.2 Bidder IT networks processing Bank Information must be monitored. Monitoring must include the following information security events:

4.2.1 Unauthorised access and unsuccessful access attempts; and

4.2.2 Third party access to Bank Information.

4.3 Bidders must ensure that Bank Information is stored and processed on internal networks located within the UK.

4.4 If a need arises to transfer Bank Information to a foreign jurisdiction on either an internal network or external network operated by a third party, the Bidder should submit a request to the Bank. For the avoidance of doubt, the Bidder should not proceed without the Bank's prior written consent having been provided.

5. Access Management

5.1 Bidders will be able to use their internal IT systems to process Bank Information during the Procurement subject to meeting the specific requirements set out in this paragraph 5. Bidder IT systems processing Bank Information must;

5.1.1 assign a unique user identifier to each user;
5.1.2 not display or store passwords in clear text during login;
5.1.3 authenticate the user before access is provided;
5.1.4 not display error or help messages that would facilitate an unauthorised access attempt;
5.1.5 lockout users after five (or less) consecutive unsuccessful authentication attempts until an administrator is authorised to re-enable the user;
5.1.6 lock the user's screen after a reasonable period of inactivity forcing re-authentication;
5.1.7 ensure users access to IT systems follows industry good practice;
5.1.8 force passwords to be changed if they have been set by administrators.

5.2 Passwords for Bidder IT systems must follow industry good practice:

5.2.1 be different from their associated unique identifier;
5.2.2 contain characters from at least three of the following:
5.2.2.1 numbers;
5.2.2.2 upper case letters;
5.2.2.3 lower case letters;
5.2.2.4 special characters (e.g. &^%);
5.2.3 forced to change on first login, and provided by an administrator.

5.3 The Bidder must ensure the following requirements are adhered to by Staff:

5.3.1 confirm that the relevant Staff member has access only to the Information required to complete their current role on the Procurement;
5.3.2 validate the access permissions for each Staff member;
5.3.3 confirm that segregation of duties and least privileged principles are maintained;
5.3.4 identify and disable any accounts where a member of Staff has taken a long term leave of absence, left the Bidder's organisation or is no longer involved in the Bidders participation in the Procurement;
5.3.5 remove or disable any dormant account that has not been accessed for more than 90 days; and
5.3.6 retain evidence that Staff entitlement reviews have taken place.

5.4 Bidders will be required to come on to Bank premises to view Information that the Bank deems to be of Bank Secret (or above) classification and too sensitive to share electronically. Where the Bidders Staff require access to Bank Secret Information, the following will apply:

5.4.1 access will take place in a secure data room on Bank premises;
5.4.2 access will be facilitated by Bank staff;
5.4.3 access will be paper based as a principle and stored/processed on a secured PC on Bank premises by exception;
5.4.4 an Information Security log will be maintained noting Bidder Staff access, location and the deletion/destruction of the Bank Information recorded.

5.5 Bidders must ensure that its Staff dispose of Bank Information securely by:

5.5.1 erasing electronic Bank Information such that the information cannot be retrieved, through the use of accredited products such as Overwrite, Secure Erasure (ATA hard disks only), Degaussing or by physical device destruction;
5.5.2 shredding hard-copy Bank Information using a cross-cut shredder to a level that the document may not be reconstituted;

5.5.3 obtaining a certificate of destruction when using a third party to dispose of Bank Information;

5.5.4 maintaining an audit log of the disposal of electronic and physical documents to validate destruction.

5.6 Bidders must **not** use removable media devices to store or transfer Bank Secret or Top Secret Information. Bidders must not use removable media devices to store or transfer Bank Confidential Information unless approved by the Bank in advance. In identifying a requirement to store or transfer Bank Confidential Information on removable media, Bidders must ensure the following;

5.6.1 control access to removable media is read-only;

5.6.2 only store Bank Confidential Information on removable media using approved encryption mechanisms;

5.6.3 maintain an audit log of Bank Confidential Information that is copied to or accessed from the removable media.

5.7 Bidders must ensure that its Staff's access to any online information sharing portals (i.e. ProContract) is managed in accordance with 'need to know' and 'least privilege' principles;

5.7.1 All Staff accessing information sharing portals used by the Bank during the Procurement must be part of the Bid Team and as such have been SC cleared;

5.7.2 All access to information sharing portals must be conducted from Bidder IT systems located in the UK as detailed in section 4.3;

5.7.3 All Staff must adhere to the password requirements as detailed in section 5.2 and must have two-factor authentication enabled.

6. Network and Communications Security

6.1 Bidders must ensure that any Bank Information they intend to share externally e.g. information transfer to a sub-contractor, the Bank is notified in advance and gives their approval prior to transfer.

6.2 Bidders must maintain segregation between Bank Information and other information owned by the Bidder or third parties stored on the Bidder's IT network. This segregation must;

6.2.1 ensure access control to Bank Information is restricted to Staff on the Bid Team (or those that Bank Information is shared with in accordance with paragraph 3.2);

6.2.2 ensure Staff only have access to the documents they need for their role;

6.3 Bidders must produce audit logs recording user activities, system administrator, exceptions, and information security events at the document level, which shall be kept for a reasonable period of time (or such period as notified by the Bank), to assist in future investigations and access control monitoring.

6.4 Where there is a requirement to send information to the Bank over email, the Bidder must use approved encryption mechanisms to send this information securely. For information, the Bank recognises the following approved industry standard mechanisms: PGP, TLS, SSL V3.0.

7. Management of sub-contractors

7.1 Bidders must inform the Bank of any intention to employ the services of an external third party including sub-contractors to support their participation in the Procurement. Any decision to employ an external third party must be approved by the Bank in the first instance.

7.2 Bidders must ensure that all sub-contractors adhere to the Security Requirements, set out in this document, and that these are implemented, operated, and maintained by all sub-contractors at all times in connection with any Bank Information in their possession or control. The Bank may require any sub-contractors to enter into non-disclosure agreements with the Bank prior to any Bank Information being shared.

7.3 Bidders must maintain inventories of external third parties to whom they provide access to Bank Information. This includes information stored in cloud-based systems owned or operated by sub-contractors. The inventories must record:

7.3.1 the name of each third party, the reason for such access to Bank Information and the name of the individual at the Bidder responsible for the relationship with the third party;

7.3.2 access, transfer or storage details for Bank Information.

7.3.3 the extent of the access that each external third party has to any IT systems used by the Bidder (including cloud-based systems) in regards to their participation in the Procurement.

Appendix A – Bank Information Classification Scheme

Classification	Unclassified	Bank Confidential	Bank Secret & Top Secret
Definition	The compromise of this information or material would have no effect or only a minor effect. In a worst case scenario this would be no more than one or more of the following: • little adverse effect on the Bank, individuals, HMG, the City or financial markets; • minor inconvenience to any party; • minor inconvenience to any party; • no risk to any party's personal safety; • minor financial loss to any party; • minor damage to any party's standing or reputation; • minor distress to any party; • no assistance in the commission of, or hindrance to, the detection of crime.	The compromise of this information would be likely to cause one or more of the following: • materially damage the reputation of the Bank; • damage the operational efficiency of the City, the economy, or financial markets; • cause distress to individuals; • breach proper undertakings to maintain the confidence of information provided by third parties (likely to include all customer data and individual institutions data); • breach statutory restrictions on the disclosure of information including all personal information (staff, customer or other) subject to the Data Protection Act or GDPR; • Facilitate improper gain or advantage for individuals or companies, impede the investigation, or facilitate the commission of crime.	The compromise of this information or material would be likely to cause one or more of the following: • serious damage to the reputation of the Bank; • substantial damage to the City, the economy, or financial markets; • cause serious damage to Bank relations with HMG; • prejudice individual security or liberty; • impede the investigation or facilitate the commission of serious crime.
General Examples	• Public Domain Data	• Personal staff information including any information pertaining to Bank staff involved in the Procurement; • Analysis of Proof-of-Concept materials; • Business and System Design documentation; • Business and System Requirements documentation; • Agendas and Papers for Meetings related to the Procurement; • Personal notebooks containing any of the materials above.	• Sensitive Business and System Design documentation of critical system components.