

***INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) INFRASTRUCTURE AND SECURITY STANDARDS***

INFORMATION TO BE PROVIDED BY APPLICANTS FOR REGISTRATION AS A PAYMENT SERVICE PROVIDER

**NAME OF COMPANY:**

***ICT INFORMATION TO BE PROVIDED BY***

***APPLICANTS FOR REGISTRATION AS A***

***PAYMENT SERVICE PROVIDER***

**Please provide the following information:**

1. **Risk-Management Framework**

|  |  |  |
| --- | --- | --- |
| **Risk-Management Framework** | **Information to be provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
| 1. What processes and systems are in place to mitigate against all material risks in your IT environment? E.g. cybersecurity, physical etc. | E.g.: Provide evidence such as: Risk Assessment Document; Policies and procedures document; Threat Management Systems: Data Loss Prevention (DLP)/Anti-Money Laundering (AML)/Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)/Log/Alert Management |  |
| 1. Provide information on your risk-management framework. | E.g.: Control Objectives for Information and Related Technology (COBIT) |  |
| 1. Do you require any third party providers in daily operations? If yes, what policies/procedures are in place to manage the risks? | E.g.: Service Level Agreement (SLA)/Non-Disclosure Agreement (NDA)/Report demonstrating the security, reliability and resilience of the third parties’ operations and its assessment. |  |
| 1. How is the overall security posture evaluated? | E.g. Internal/External Threat Assessment Evidence: Vulnerability Assessment Report; Penetration Tests Reports; Security Policy |  |
| 1. What are the identified timelines for dealing with detected risks/threats? | E.g.  Timelines for addressing threats for clearly identified severity levels such as low medium and high |  |

1. **Information Security Framework**

|  |  |  |
| --- | --- | --- |
| **Information Security Framework** | **Information to be provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
| 1. What mechanisms are in place to ensure your ICT infrastructure is physically secure? | E.g.: Locked cabinets; authorized access to data center |  |
| 1. Please provide information on the following:   -Data storage and its security E.g. cloud storage; SAN/NAS  -Transactional data transmission  -Authentication level for external access  -Backups/recovery solution | E.g.: Encryption; Data retention policy  Online: (Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) Certificates/Encryption)  Two factor authentication |  |
| 1. Has stress testing analysis been performed on the technology platform solution? How often will this review/test be performed?  In situations where the maximum capacity is exceeded, what plans are in place to address this? | E.g.: Stress Testing Analysis |  |
| 1. Identify change management processes and the management involvement in same? | E.g.: Change management processes |  |
| 1. Identify how the safeguarding of customer information stored on database servers are secured. | E.g.: Separation of database and web application servers  Utilization of dedicated VPN connection  Use of firewalls |  |

1. **Reliability/Resilience of Systems**

|  |  |  |
| --- | --- | --- |
| **Reliability/Resilience of Systems** | **Information to be provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
| 1: What are the operational availability, reliability and resilience objectives and how are these ensured? | E.g.: Evidence/information on operational objectives and environment, processes and procedures that support the objectives.  E.g.: strategic plan, mission statement, operational guidelines and procedures, technology systems details including list of hardware and software used, network/system diagrams, employee details – skills, functions, roles and numbers; third party IT providers inclusive of service contracts |  |
| 2: How are operations protected against natural disasters, power failures, and adverse human actions? | E.g.: Evidence/information on technical environment, processes and procedures with respect to risk assessments and mitigation for natural disasters, etc.  E.g: technology and operational risk management procedures and guidelines. |  |
| **Operations monitoring and incident management** |  |  |
| 3: How are operations and incidents identified, monitored, recorded, categorized, analyzed and managed (including escalation/reporting)? | E.g.: Evidence/information on fraud monitoring/AML and incident review processes.  E.g.: incident management (or helpdesk) process, procedures, guidelines or details |  |
| 4: What is the process to ensure incidents do not recur in the future? | E.g.: Evidence/information on process/procedures to be performed as a post-mortem of incidents and identification of the root cause of problems to avoid recurrence. E.g.: risk management and assessment guidelines, procedures, problem management etc. |  |
| **Business continuity** |  |  |
| 5: What are the business continuity and disaster recovery objectives?  How frequently will these objectives be reviewed by management? | E.g.: Evidence/information on business continuity and disaster recovery processes and procedures.  E.g.: Disaster Recovery plan, procedures/ guidelines, Business Continuity plan, procedures/guidelines. |  |
| **Business continuity (Cont’d)** |  |  |
| 6: What is the communication plan to handle disasters? | E.g.: Evidence/information on processes and procedures used to communicate to stakeholders in the event of a disaster.  E.g.: Communication process/procedure/guidelines to stakeholders |  |
| **Software update/upgrade** |  |  |
| 1. What is the plan and timelines for the replacement of critical software approaching identified end of life termination of vendor support? |  |  |
| **Technology Platform support - Staffing** |  |  |
| 1. What staffing resources have been allocated in support of the technology platform? | E.g.: the number and skills of personnel required to administer and maintain the technology solution on a daily basis  E.g.: Helpdesk support |  |
| **End User Guides** |  |  |
| 1. What end user guides exist of agents and users of the System? |  |  |

1. **Technology Planning**

|  |  |  |
| --- | --- | --- |
| **Technology Planning** | **Information to be provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
| 1: What are the processes, policies, procedures and governance methods in place for technology planning? | E.g.: Evidence/information on the policies, processes and procedures in place to address the lifecycle use of technologies.  E.g.: Technology acquisition and hardware replacement (lifecycle) details, certifications or documents showing alliances with appropriate governance bodies/institutions, etc. (Information Technology Infrastructure Library (ITIL)/ International Organization for Standardization (ISO)/COBIT). Strategy in place which addresses how acquire/maintain/replace hardware/software. |  |
| 2: How are technology risks such as, obsolescence risks and information security risks handled? | E.g.: Evidence/information on processes and procedures in place to assess and address technology risks such as obsolescence.  e.g. technology risk management details/process/procedure, lifecycle details, vulnerability and patch management details/procedures/guidelines. |  |
| 3: What are processes, policies, procedures, and governance methods for implementing changes to the technologies used? | E.g.: Evidence/information on change management procedures including risk assessment and review before a change to the infrastructure or procedures.  e.g. change management process/procedures, technology risk management plan |  |
| 4: How are any proposed important changes to technology communicated to relevant stakeholders? | E.g.: Provide evidence/information on processes and procedures used to communicate to stakeholders in the event of a service disruption.  e.g. communication plan. |  |

1. **Communication**

|  |  |  |
| --- | --- | --- |
| **Communication** | **Information to be provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
| 1. State the communication medium to be used for each process in the life cycle of the transactions from initiation to final confirmation. | E.g.: Provide information on each step in the life cycle indicating the media used to communicate e.g. email, physical receipt, electronic statements etc. |  |
| 1. How would information be disseminated to the users in terms of their roles and responsibilities as participants? Will user guides be issued? How will users provide feedback to the Applicant in terms of questions, complaints and requests for support? | E.g.:   * Education Policy/guideline and awareness programs * Customer support service or helpdesk * Website * Circulars |  |
| 1. If there are operational changes, how are the users notified? | E.g.: Communication medium e.g. phone calls, emails, public notices etc. |  |
| 1. How are the systems risks documented and shared? For e.g. potential losses if the system is compromised. | E.g.: Terms of agreement; contract; disclaimers etc. |  |
| **Communications on incidents and crisis.** |  |  |
| 1. How do the users and Central Bank get notified about incidents e.g. if the system or user information appears to be compromised? | E.g.: Form of electronic/secure medium (E.g.: encrypted email; text message; phone call, popup messages) |  |
| **Communications with the Payment Authority** |  |  |
| 1. What is the plan to address communication between Applicant and Central Bank inclusive of operational and system changes? | E.g.: Plan for provisions for regular reporting on system health; new releases updates; handling fraudulent activities; change proposal document |  |

1. **Additional ICT Information provided**

|  |  |  |
| --- | --- | --- |
|  | **Information Provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Additional ICT Information provided**

|  |  |  |
| --- | --- | --- |
|  | **Information Provided** | **Details / Documents Provided / Reference (Please detail responses and list all documents submitted)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |