INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) OUTSOURCING QUESTIONNAIRE

NAME OF COMPANY:

INFORMATION AND COMMUNICATIONS TECHNOLOGY OUTSOURCING QUESTIONNAIRE

Name of Respondent: _____

Designation/Title: _____

Phone Number: _____

Email Address: _____

Date:

Instructions:

1) This questionnaire is to be completed by officers who have direct knowledge of the institution's technology operations and systems. The response should be verified by the officer's superior.

2) The most recent information should be provided. For items that are not applicable, please indicate with "N/A".

3) Attachments should be included where appropriate.

GENERAL COMPANY INFORMATION

A. BUSINESS MODEL AND OBJECTIVES

1) Describe the company's business model.

2) What are the company's business objectives?

3) How does the Information and Communication Technology (ICT) system meet the business objectives?

4) Who are the business' customers/system users?

5) Who are the business' e-commerce customers?

6) What are the available system performance and reliability?

7) What information (both incoming and outgoing) is required by the organisation?

B. OUTSOURCING ARRANGEMENT DETAILS (IF APPLICABLE)

1) Please describe your outsourcing arrangement(s)? (Example: Is the outsourcing arrangement a cloud computing arrangement?)

2) List all the proposed activities and operations to be outsourced and indicate whether the outsourced activity is critical to the business or not.

Activity #	Service(s) to be outsourced	Critical (Y/N)

3) Indicate who provides the outsourced activities as indicated in Question 2 above and the location of each service provider.

Activity #	Service Provider	Location

4) Are there service level agreements for each of the activities outsourced (as indicated in Question 2)?

Yes ☐ (Please attach the agreements)

No ☐

If "No", please explain:

C. INFORMATION COLLECTION AND SECURITY

1) What information is entered into the system?

2) What information is generated by the system?

3) What information is processed by the system?

4) What information is stored in the system?

5) What information is retrieved by the system?

6) How important is the information to the business objectives?

7) What is the sensitivity/classification level of the information in Questions 1 – 7 above?

8) Where specifically is the information processed and stored?

9) Is there any other party that has access to any of this information? If so, please provide details on who can access the information and for what reason.

10) Describe the paths of information flow and the security arrangements to accommodate this.

11) For your organisation's data residing with the Service Provider, what are the backup and recovery arrangements? Have you jointly tailored and tested this with your Service provider? Please provide details and/or relevant documentation/test results.

D. RISK ASSESSMENT AND MANAGEMENT

1) Has your organisation performed a risk assessment of this outsourcing arrangement, including security risk assessment against the latest security threats? Please elaborate on the key risks and threats that have been identified for this/the outsourcing arrangement(s) and the action(s) that have been or will be taken to address them.

2) If the outsourcing arrangement requires system connectivity between your organisation and the Service Provider, how does your organisation protect your networks and systems from the potential threats arising from the system connectivity?

3) If the outsourcing arrangement involves the processing or storage of any sensitive information at the Service Provider, how does your organisation address the risk of unauthorised disclosure as well as intentional or unintentional leakage of that information? Please provide details of the preventive and detective measures in place, if any.

4) Does the Service Provider employ a system architecture that involves multi-tenancy and data commingling for the outsourced service(s)? If so, how are the associated risks addressed?

5) Are the outsourced operations using hardware (i.e. servers/network devices) dedicated to the organization?

E. IT SECURITY

1) Are the following security practices implemented by the Service Provider?

Security Practices	Yes	No
i. Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.		
ii. Install firewalls between internal and external networks as well as between geographically separate sites.		
iii. Install intrusion detection-prevention devices (including denial-of-service security appliances where appropriate).		
iv. Develop built-in redundancies for single point of failure which can bring down the entire network.		
v. Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities. If yes, provide: Frequency of application security reviews: _____ Date of last application security review: _____(DD/MM/YY) Name of firm which conducted the review: _____ Please attach a copy of the application security review results.		
vi. Engage independent security specialists to assess the strengths and weaknesses of internet facing applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff. If yes, provide: Frequency of assessment: _____ Date of last assessment: _____(DD/MM/YY) Name of firm which conducted the assessment: _____ Please attach a copy of the assessment results.		

Security Practices	Yes	No
vii. Conduct penetration testing at least annually. If yes, provide: Frequency of penetration tests: _____ Date of last penetration test: _____(DD/MM/YY) Name of firm which conducted the test: _____ Please attach a copy of the penetration test results.		
viii. Establish network surveillance and security monitoring procedures with the use of network scanners, intrusion detectors and security alerts.		
ix. Implement anti-virus software and apply updates regularly. If yes, provide: Frequency of anti-virus updates: _____ Date of last anti-virus update: _____(DD/MM/YY) Name of firm which conducted the update: _____ Please attach a copy of the anti-virus update results.		
x. Conduct regular system and network configurations review and data integrity checks. If yes, provide: Frequency of reviews and checks: _____ Date of last review and check: _____(DD/MM/YY) Name of firm which conducted the review and check: _____ Please attach a copy of the review and check results.		
xi. Maintain access security logs and audit trails.		
xii. Analyse security logs for suspicious traffic and intrusion attempts. If yes, provide: Frequency of analysis: _____ Date of last analysis: _____(DD/MM/YY) Name of firm which conducted the analysis: _____ Please attach a copy of the analysis results.		
xiii. Establish an incident management and response plan.		

Security Practices	Yes	No
xiv. Test the predetermined response plan relating to security incidents. If yes, provide: Frequency of testing: _____ Date of last test: _____(DD/MM/YY) Name of firm which conducted the test: _____ Please attach a copy of the test results.		
xv. Install network analysers which can assist in determining the nature of an attack and help in containing such an attack.		
xvi. Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.		
xvii. Maintain a rapid recovery capability.		
xviii. Conduct security awareness education and programs. If yes, provide: Frequency of awareness conduction: _____ Date of last awareness conduction: _____(DD/MM/YY) Name of firm which performed the awareness conduction: _____		
xix. Require frequent ICT audits to be conducted by security professionals or internal auditors who have the requisite skills. If yes, provide: Frequency of anti-virus updates: _____ Date of last anti-virus update: _____(DD/MM/YY) Name of firm which conducted the update: _____ Please attach a copy of the anti-virus update results.		
xx. Consider taking insurance cover for various insurable risks, including recovery and restitution costs.		
xxi. Provide separate physical/logical environments for systems development, testing, staging and production; connect only the production environment to the internet.		
xxii. Implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.		
xxiii. Implement two-factor authentication at login for all types of online systems, such as internet banking, online trading platforms, insurance portals for policyholders as well as a specific OTP or digital signature for each value transaction above a specified amount selectable by the customer or predetermined by your organisation.		

	Security Practices	Yes	No
xxiv.	Deploy strong cryptography and end-to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.		
xxv.	Encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.		
xxvi.	Deploy strong user authentication in wireless local area networks and protect sensitive data with strong encryption and integrity controls.		

If you answered "No" to any of the above, please indicate why.

i. PROTECTION OF INFORMATION

2) Have you obtained from the Service Provider a written undertaking to protect and maintain the confidentiality of your data? Please attach the relevant documentation.

3) Is the Service Provider able to isolate and clearly identify your data (e.g. customer data, documents, records and assets) to protect their confidentiality? Please explain how your data can be isolated and identified.

4) Is encryption implemented to protect the transmission of data (example: PINs)? What type of encryption is implemented? If no, please explain why.

5) What other security controls are put in place to protect the transmission and storage of (sensitive) production and backup data (e.g. customer data) within the infrastructure of the Service Provider?

6) Are there procedures established to securely destroy or remove the organisation's production and backup data stored at the Service Provider when the need arises? Please elaborate.

ii. DATA CENTRE PHYSICAL AND ENVIRONMENTAL CONTROLS

7) Where are the data centre(s) of the Service Provider located? Indicate the data centre(s) in which your organisation's sensitive data would be stored and/or processed.

No.	Locations of Data Centre	Storing your organisation's data (Y/N)

8) Was/Were the data centre(s) listed above officially rated?

No.	Data Centre	Data Centre Evaluator	Classification of Data Centre : Tier I, II, III, IV

9) Have you obtained a report on the Threat and Vulnerability Risk Assessment on the physical security and environmental controls of the data centre(s)? (Please attach the report.) What were the key risks and security issues raised, and how were they addressed?

iii. USER AUTHENTICATION AND ACCESS MANAGEMENT

10) Does the Service Provider have privileged access or remote access to perform system/user administration for the outsourced service? If so, does the Service Provider have access to your organisation's sensitive data? Please provide details on the controls implemented to mitigate the risks of unauthorised access to sensitive data by the Service Provider, or other parties.

11) Are the following controls and measures put in place at/by the Service Provider?

	Controls & Measures	Yes	No	Frequency
i.	The activities of privileged accounts are logged and reviewed regularly.			
ii.	Audit and activity logs are protected against tampering by privileged users.			
iii.	Access to sensitive files, commands and services are restricted and protected from manipulation.			
iv.	Integrity checks are implemented to detect unauthorised changes to databases, files, programs and system configuration.			
v.	Password controls for the outsourced systems and applications are reviewed for compliance on a regular basis.			
vi.	Access rights for the outsourced systems and applications are reviewed for compliance on a regular basis.			

If you answered "No" to any of the above, please explain:

F. EXIT STRATEGY

1) Please explain the contingency plan for replacing the Service Provider in the event of its cessation.

2) Please provide details on your right to terminate the Service Level Agreement in the event of default, ownership change, insolvency, change of security or serious deterioration of service quality.

3) Explain if you able to have all information and assets promptly removed or destroyed in the event of contract termination with the service provider, either on expiry or prematurely.

CLOUD SPECIFIC INFORMATION

1) Is the information stored and processed in the cloud?

2) Who is the cloud owned by and where is the owner located?

3) What regulations are the cloud and information in the cloud subjected to?

4) What type of cloud is it? (Example: private, public, hybrid)

5) Who else has access to the cloud and the information stored within it?

6) Do other companies that you provide services to utilise the same cloud? How it is ensured that they can only access their data and not another company's data?

7) Please indicate by who each of the following activities/services are managed by use of the key below.[1]

Managed by	**Abbreviation/Key**
You, The entity	E
The Outsourced Provider	O
Both You and the Outsourced Provider	S

	Activity/Service	**IaaS**	**PaaS**	**SaaS**
1.	Install and maintain a firewall configuration to protect data.			
2.	Do not use outsourced provider-supplied defaults for system passwords and other security parameters.			
3.	Protect stored data.			
4.	Encrypt transmission of data across open, public networks.			
5.	Protect all systems against malware and regularly update anti-virus software or programs.			
6.	Develop and maintain secure systems and applications.			
7.	Restrict access to data by business need to know.			
8.	Identify and authenticate access to system components.			
9.	Restrict physical access to data.			
10.	Track and monitor all access to network resources and data.			
11.	Regularly test security systems and processes.			
12.	Maintain a policy that addresses information security for all personnel.			

[1] Source: PCI SSC Cloud Computing Guidelines

APPENDIX I – SERVICE PROVIDER SELECTION CRITERIA & DUE DILIGENCE

1) Is the Service Provider selection process formally defined and documented?

Yes ☐

No ☐

If "Yes", please provide documentation; otherwise if "No", please explain:

2) Do the selection criteria consider the following?

	Criteria	Yes	No
i.	Competence and experience of the Service Provider		
ii.	Past track-records		
iii.	The Service Provider's staff hiring and screening process		
iv.	Financial strength of the Service Provider (i.e., assessment of the past 3 years audited financial statements and other relevant information)		
v.	Inputs from the Service Provider's previous/existing customers and/or independent parties (i.e., complaints, compliance, pending litigation, business reputation)		
vi.	Business resumption and contingency plan		
vii.	Security and internal controls, audit, reporting and monitoring		
viii.	Strength of parent company support		

If "No", please explain:

3) Apart from the current Service Provider, have other vendors been considered?

Yes ☐

No ☐

If "Yes", state the name of vendor(s) and reason(s) for not selecting them:

If you answered "No", please explain:

4) Explain why the current service provider was chosen.
