

Cloud Computing Appendix C

|  |  |
| --- | --- |
| Cloud Computing Service Provider(s) Information\*  *Scope:*   * *“Vendor(s)” - Service provider(s) providing the cloud service solution.* * *“Cloud Service Provider(s) (“CSP(s)” - Cloud platform provider(s) behind the cloud service solution (e.g. Microsoft Azure, Amazon AWS, Oracle Cloud, etc.)* * *Other application provider(s), if any.*   *\*Please duplicate this table for solution when there are more than one Vendor(s), CSP(s) or other application provider(s)..* | |
| **Vendor** | |
| **Name of Vendor:** | *[Vendor Name]* |
| **Vendor website:** | *[Vendor Website]* |
| **Vendor background, size, and major business:** | *[Description]* |
| **Vendor business location:** | *[Vendor business office address]* |
| **Number of Employees:** | *[Employee no., both local and worldwide]* |
| **Major Customer Coverage:** | *[Description]* |
| **Vendor background and experience with Hutchison Group/CKHH (if any):** | *[Description]* |
| **Vendor roles and responsibilities, as well as involvement in this project:** | *[Description]* |
| **Cloud Service Provider (CSP)** | |
| Select the applicable CSP below  Microsoft Azure  Amazon Web Services  Oracle Cloud  Others.  *When option “Others” is selected, please also fill in the following details of the Vendor.* | |
| **Name of CSP:** | *[CSP Name]* |
| **CSP website:** | *[CSP Website]* |
| **CSP background, size, and major business:** | *[Description]* |
| **CSP business location:** | *[CSP business office address]* |
| **Number of Employees:** | *[Employee no., both local and worldwide]* |
| **Major Customer Coverage:** | *[Description]* |
| **CSP background and experience with Hutchison Group/CKHH (if any):** | *[Description]* |
| **CSP roles and responsibilities, as well as involvement in this project:** | *[Description]* |

| **#** | **Supplementary information** | **(Y/N)** |
| --- | --- | --- |
| **Policies and Procedures** | | |
|  | Indicate whether the Vendor(s) has policies and procedures covering information security domains under industry best practice. |  |
| **Application Development and Security** | | |
|  | Describe the security controls or mechanism(s) adopted by this solution to enforce the protection and integrity of Hutchison Ports data. |  |
|  | Indicate ownership rights to the data hosted within the solution. |  |
|  | Explain the security practices followed during application development and the development lifecycle. |  |
| **Data, Media, and Key protection** | | |
|  | List all personal, financial and payment card-related data and all their related data flows in the solution. |  |
|  | For all personal data provided in Q5 (if any), describe the security control(s) or mechanism(s) in place to protect this data during storage, use and transmission. |  |
|  | For all other data provided in Q5, describe the security control(s) or mechanism(s), when different than Q6, to enforce protection of data during storage, use and transmission. |  |
|  | Explain the overall cryptographic key management practices. |  |
|  | Explain the treatment of data, data transfer process and data destruction process when the business relationship expires, along with how Vendor(s) provide assurance for completeness of these processes. |  |
|  | Explain if there are control(s) and/or tool(s) to prevent data transfer to any business entities or countries without Hutchison Ports' consent or notice. Explain how Hutchison Ports is able to control access to data and monitor access logs to data. |  |
| **Cloud Infrastructure Security** | | |
|  | Provide the vulnerability management procedures followed by the Vendor(s) to address any identified security vulnerabilities, in terms of detection and treatment practices. |  |
|  | Explain how Vendor(s) align their vulnerability management procedures with that of Hutchison Ports when addressing any security vulnerabilities that would require collaboration of both parties, specifically on notification and response. |  |
|  | Describe the approach used by Vendor(s) / CSP(s) to separate the Hutchison Ports data from other service customers' data. |  |
|  | Describe the access authentication method(s) or mechanisms that will be put in place. |  |
|  | Describe the logging and monitoring capability of this solution. |  |
|  | Describe how the Vendor(s) manage the security of cloud infrastructure and its virtual machines (“VM”) or platforms. |  |
| **Identity and Access Management** | | |
|  | Explain how identities, and user and privileged accounts are managed by the solution. |  |
| **Personnel Security** | | |
|  | Explain the Vendor(s) personnel security practices that have been adopted. |  |
| **Business Continuity and Incident Response** | | |
|  | Explain what control(s) or mechanism(s) are in place to meet Hutchison Ports resilience requirements (e.g. can the Vendor(s) guarantee the system will be available if required in an emergency?). |  |
|  | Explain if the Vendor(s) has a defined and documented method for determining the impact of any disruption to them. |  |
|  | Explain the business continuity management practices adopted by the Vendor(s). |  |
| **GRC and Audit** | | |
|  | Indicate whether a security control framework is maintained by the Vendor(s) in maintaining compliance to any identified Information System regulations. |  |
|  | Explain how Hutchison Ports evaluate requirement in the data location, relevant legal and regulatory requirements, for any data that is involved in the solution. |  |
|  | Explain if the Vendor(s) has performed risk assessment(s) or audit(s) on their security operations on at least an annual basis. |  |
| **Third Party Risk Management and Protocols** | | |
|  | Provide the third-party assurance reports available for each layer (e.g. physical data centre layer, infrastructure layer, application layer) of the solution’s technology stack. |  |
|  | Describe the support process(es) for audits, forensic or legal discovery provided by the Vendor(s). |  |
|  | Explain on how CSP(s) would manage and communicate changes to the Vendor(s). Explain also if the Vendor(s) would perform any third-party audits or reviews on the CSP(s) on a regular basis. |  |
|  | Explain controls or procedures to resolve data interoperability and portability concerns. |  |
| **Remote Access Security** | | |
|  | Describe practices adopted for mobile security, in terms of awareness training, inventory management, mobile device management, encryption, password policies enforcement, deployment of security patches. |  |

|  |  |
| --- | --- |
| **Supporting Documents** | **Y/N** |
| 1. Third party information security risk assessment report - Includes rating, finding, and mitigating controls) and management approval. *Common framework and reports are ISO27017, NIST, COBIT, SSAE16, ISAE3402, SOC2, PCI DSS, CSA CCM, etc.* |  |
| 1. Self-Risk Assessment Result |  |
| 1. Solution and/or Network Architecture/Design documents and diagrams |  |
| 1. Application Architecture Diagram (if applicable) |  |
| 1. Data Flow Diagram |  |
| 1. Recent Vulnerability Scanning Report and Penetration Test Result |  |
| 1. Service agreement |  |
| 1. Application code scanning report    * Static application security testing (SAST) scanning report    * Dynamic application security testing (DAST) scanning report |  |
| 1. BU data processor and/or legal review supporting document (e.g. email, etc.) if personal data involved. |  |

**Appendix II - Supplementary information for Cloud Computing Checklist ()**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Area** | **#** | **Supplementary information** | | |
| **Policies and Procedures** |  | **Provide if the Vendor(s) have the latest certificates under industry best practice framework, e.g.**   1. **Certificate of approval, issued by a third party; and/or** 2. **Risk assessment performed by a third party** | | |
| **Certificate of approval, issued by a third party; and/or**  ISO/IEC 27017  American Institute of Certified Public Accountants’ (AICPA’s) Service Organisation Controls (SOC) 2  Cloud Security Alliance's (CSA’s) Cloud Controls Matrix (CCM)  Others, please specify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *Please attached it in the “Supporting Documents” section above.*  If no certificate is available, please proceed to the following supplementary question. | | |
| **For the Vendor(s), indicate whether the following domains are covered in their policies and procedures,** | **Y/N** | **Remarks, if any** |
| 1. Asset Management |  |  |
| 1. Backup Management |  |  |
| 1. Baseline security |  |  |
| 1. Business Continuity |  |  |
| 1. Change & Configuration Management |  |  |
| 1. Data and Retention Management |  |  |
| 1. Endpoint Security |  |  |
| 1. Identity and Access Management |  |  |
| 1. Incident Response |  |  |
| 1. Key Management |  |  |
| 1. Network Operations |  |  |
| 1. People Resources |  |  |
| 1. Risk Management |  |  |
| 1. Secure Development |  |  |
| 1. Security Governance |  |  |
| 1. Service Lifecycle Management |  |  |
| 1. Systems Logging and Monitoring |  |  |
| 1. Third Party Management |  |  |
| 1. Training and Awareness |  |  |
| 1. Vulnerability Management |  |  |

|  |  |  |
| --- | --- | --- |
| **Application Development and Security** |  | **Describe what kind of security controls or mechanism(s), in relation to protection of integrity for Hutchison Ports data, are provided by this solution.**   * Web application firewall (WAF) * Data loss protection (DLP) * Intrusion Detection system (IDS) * Anti DDoS * Container Security * Cloud Security Posture Management tools (CSPM) |
| **Answer:** *[Please fill in your response]* |
|  | **For any data involved in the solution, indicate the data ownership. This should align with what is mentioned in the formal written agreement.**  *If applicable, please indicate the relevant sections when included in the service agreement.* |
| **Answer:** *[Please fill in your response]* |
|  | **During secure application development process, explain if:**   1. Software code is developed in accordance with any industry standards to enhance application security by identifying most critical risks facing organizations. Please also specify the standards followed (e.g. OWASP for web applications) and provide the *static* application security testing (SAST) scanning report (if any). 2. Dynamic application security testing (DAST) represents a non-functional testing process to identify security weaknesses and vulnerabilities in running web application. DAST scans the entire application, as well as other APIs and web services your application uses, to check if well-known attack techniques are possible. Please provide the scanning report (if any). 3. Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defences which attackers could take advantage of. Please provide the scanning report (if any). 4. Defined DevSecOps, quality change management control(s) and testing processes are in place prior production deployment. |
| **Answer:** *[Please fill in your response]* |
| **Data, Media and Key protection** |  | **List all personal data, payment card data, or financial data that would be hosted in the cloud. If this is not applicable, please explain.**   1. provide data flows diagram involved for each data type 2. provide any other third-parties (which not mentioned in above “Cloud Computing Service Provider(s) Information” section) involved in each data flow |
| **Answer:** *[Please fill in your response]* |
|  | **For any personal data provided in Q5, describe the security controls or mechanism(s) provided by the solution to protect the confidentiality, integrity and availability of our data, including data during:**   1. storage (e.g. file servers, databases, and end-user workstations, etc) 2. use (e.g. computer memory) 3. transmission (e.g. system interfaces, over public networks, and electronic messaging, etc) |
| **Answer:** *[Please fill in your response]* |
|  | **For all other data provided in Q5, describe the security controls or mechanism(s) provided by the solution to protect the confidentiality, integrity and availability of our data, including data during:**   1. storage (e.g. file servers, databases, and end-user workstations, etc) 2. use (e.g. computer memory) 3. transmission (e.g. system interfaces, over public networks, and electronic messaging, etc)   *If the controls are equivalent to what has been provided in Q6, please indicate so and proceed to the next question.* |
| **Answer:** *[Please fill in your response]* |
|  | **Explain the overall key management procedures, including at a minimum:**   1. Roles and responsibilities in key lifecycle management from generation to revocation (e.g. adoption of AWS CloudHSM, Azure [Key Vault](https://azure.microsoft.com/services/key-vault/), managed by other vendors, etc) 2. Cryptographic protocol design and algorithms supported, including the following: - Asymmetric encryption algorithm(s) - Symmetric encryption algorithm(s) - Hashing algorithm(s) *For our baseline standards on algorithms, please refer to Appendix IV.* 3. Access controls and procedures for secure key generation and to key storage 4. Communication protocol to inform Hutchison Ports for any changes in cryptosystems.   *For additional reference, please refer to Appendix IV of this document.* |
| **Answer:** *[Please fill in your response]* |
|  | **When our business relationship with the vendor expires, what are the processes for:**   1. Treatment of our data and data transfer from the Vendor(s) to Hutchison Ports, including information related to data format and transmission media. 2. Data destruction/ sanitization, including production and backup environment. Does the Vendor(s) follow an industry standard (such as NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, etc)   **Explain also on how the Vendor(s) would prove for the completeness of above processes to Hutchison Ports.** |
| **Answer:** *[Please fill in your response]* |
|  | **Describe whether there are controls and/or tools in-place to:**   1. Prevent data from being transferred to other business entities or countries, without Hutchison Ports' consent or notice. 2. Allow Hutchison Ports to control who has access to the data and monitor access logs to data. 3. Describe the backup and restoration process.   *If applicable, please indicate the relevant sections when included in the service agreement.* |
| **Answer:** *[Please fill in your response]* |
| **Cloud Infrastructure Security** |  | **Provide the vulnerability management procedures followed by the Vendor(s) to address any identified security vulnerabilities, with emphasis on the following criteria:**   1. Timely detection of vulnerabilities 2. Risk-based model for prioritizing remediation of identified vulnerabilities 3. Change management process for any patch or configuration changes |
| **Answer:** *[Please fill in your response]* |
|  | **Explain how the Vendor(s) align their vulnerability management processes with that of Hutchison Ports in addressing all security vulnerabilities that would require collaboration of both parties, with emphasis on the following criteria:**   1. Timely notification to Hutchison Ports upon discovery of security vulnerabilities 2. Timely response to inquiries by Hutchison Ports on potential identified vulnerabilities 3. Threat intelligence monitoring approach |
| **Answer:** *[Please fill in your response]* |
|  | **Describe the approach used by the Vendor(s) to separate the Hutchison Ports data from other service customers' data.**  *E.g. Logical separation which available in market:*   * *AWS: Identity and Access Management (IAM) rule, route 53, EC2 container server (EC2)* * *Microsoft Azure: Azure Active Directory, Azure DNS, traffic manager, Azure Container Service* |
| **Answer:** *[Please fill in your response]* |
|  | **Describe the access authentication method(s) or mechanisms that will be put in place by the solution, and who (with title) is responsible to manage this authentication system**  *E.g. User name and password, Multi-factored authentication, biometrics, token authentication, out-of-band authentication, Strong/expiable/non-shared authentication secrets* |
| **Answer:** *[Please fill in your response]* |
|  | **Describe the logging and monitoring within the solution:**   1. Type(s) of system events logged in audit log 2. Log information included in each log entry *E.g. User ID, timestamp, actions* 3. Retention period for the log. 4. Security controls or mechanism(s) in place to protect the confidentiality, integrity and availability of audit logs 5. Does the solution enable enforcement of unique user access accountability when:   - Detecting any potentially suspicious network behaviours or file integrity anomalies in both cloud and local network (e.g. IDS, SIEM, antivirus solution, etc.)  - Supporting forensic investigative capabilities in the event of a security breach |
| **Answer:** *[Please fill in your response]* |
|  | **Describe how the Vendor(s) enforce the security of cloud infrastructure and its VM(s) and platforms, especially which parties is/ are responsible for managing the infrastructure. How do they harden their infrastructure or detect changes (authorised or unauthorised)?**   1. Change detection 2. Clock synchronization 3. Compatibility of adopted vulnerability assessment tools or services 4. Restriction and monitoring of traffic between trusted and untrusted connections 5. OS hardening, especially for ports, protocols and services 6. Access control management, including least privilege, firewalls, MFA 7. Access restriction to utility programs or diagnostic and configuration ports |
| **Answer:** *[Please fill in your response]* |
| **Identity and Access Management** |  | **Explain how identities, and user and privileged accounts are managed by the solution, in particular:**   1. Who is responsible for provisioning (i.e. account creation), de-provisioning (i.e. account termination) of user account entitlements as well as modification to accounts in this solution. 2. The process for regular user profile reviews. 3. The person (with title) who are responsible for the processes in (i) and (ii). 4. Business case considerations for critical systems that would require higher levels of assurance and MFA secrets, including emergency access and personnel redundancy. (i.e. additional authentication access control for accessing strictly confidential information, such as salary, appraisal rating, business strategic information, etc.) 5. How Hutchison Ports is informed of any new third-party user access provisioning instances? |
| **Answer:** *[Please fill in your response]* |
| **Personnel Security** |  | **Explain the Vendor(s) personnel security practices and policies that have been adopted, including standards for the following topics:**   1. Background verification proportionate to business requirements and data classification 2. Clause(s) for adherence to information security policies in employment contracts 3. Regular security awareness training 4. Return of company assets upon termination 5. Signing of NDA upon termination. Please indicate the section number if this is included in the service agreement. |
| **Answer:** *[Please fill in your response]* |
| **Business Continuity and Incident Response** |  | **Explain what control(s) or mechanism(s) are in place to meet Hutchison Ports resilience requirements (e.g. can the Vendor(s) guarantee the system will be available if required in an emergency?).**  *An example of emergency situation would be the Vendor(s) suffering from major data loss.* |
| **Answer:** *[Please fill in your response]* |
|  | **Explain if the Vendor(s) has a defined and documented method for determining the impact of any disruption to Hutchison Ports. If so, please indicate if the following are covered:**   1. Identify critical products and services 2. Identify all dependencies, including processes, applications, business partners, and third party service providers 3. Understand threats to critical products and services 4. Determine impacts resulting from planned or unplanned disruptions and how these vary over time 5. Establish the maximum tolerable period for disruption 6. Establish priorities for recovery 7. Establish recovery time objectives (RTO) for resumption of critical products and services within their maximum tolerable period of disruption (i.e. in SLA) 8. Estimate the resources required for resumption   *If applicable, please indicate the relevant sections when included in the service agreement.* |
| **Answer:** *[Please fill in your response]* |
|  | **Explain the business continuity management practices adopted by the Vendor(s), e.g.:**   1. A Business Continuity Plan ("BCP") is in place and regularly reviewed 2. BCP takes into consideration environmental risks at physical operation sites 3. BCP drills are carried out on at least an annual basis |
| **Answer:** *[Please fill in your response]* |
| **GRC and Audit** |  | **Is a security control framework maintained by the Vendor(s) that includes identifying and maintaining compliance to any identified regulations, e.g.:**   1. Vendor(s) maintains a control framework which captures standards, regulatory (e.g. GDPR, PCI DSS compliance, etc), legal and statutory requirements relevant to their business needs 2. Accountable business role(s) (Vendor’s Legal Department) review the information security policy at planned intervals, such as the governance in GDPR |
| **Answer:** *[Please fill in your response]* |
|  | **Explain how would Hutchison Ports be able to evaluate requirements among data location(s) as well as any relevant legal and regulatory requirements for locations if any data are to be transmitted, stored or processed by the solution. For each location, specify whether:**   1. Local legal or regulatory requirement(s) (e.g. GDPR compliance, China Cyber Law, etc.) have been considered and addressed 2. Any cross-border requirement(s) are considered and addressed   *If applicable, please indicate the relevant sections when included in the service agreement or Hutchison Legal Team review confirmation. For additional reference, please refer to Appendix V of this document.* |
| **Answer:** *[Please fill in your response]* |
|  | **Explain if the Vendor(s) has performed any internal or external risk assessment(s) or audit(s) on the effectiveness of their security operations processes and procedures, or the security controls they have in place. Are risk assessments and audits completed at least annually.** |
| **Answer:** *[Please fill in your response]* |
| **Third Party Risk Management and Protocols** |  | **Provide the third party assurance reports available each Vendor(s) for each layer (e.g. physical data centre layer, infrastructure layer, application layer) of the solution’s technology stack.**  *Please also attach them in the "Supporting Documents" above for our review in terms of application solution and infrastructure.* |
| **Answer:** *[Please specify any reports attached or any third-party assessment(s) performed]* |
|  | **Describe the support processes in place with the Vendor(s) to support our audit, forensic or legal discovery processes, including by contractual means agreeing to:**   1. Support any potential/ regular third-party risk assessment practice carried out by Hutchison Ports. 2. Provide any relevant information about security events/incidents in a timely manner. 3. Collaborate with law enforcement in any relevant investigations.   *If applicable, please indicate the relevant sections when included in the service agreement.* |
| **Answer:** *[Please fill in your response]* |
|  | **If a CSP(s) is involved in the solution, explain:**   1. How would the CSP(s) manage and communicate changes to the Vendor(s), especially when the change(s) may impact on the Vendor(s)’ agreement made to Hutchison Ports? 2. Are there are any third-party audits or reviews carried out by the Vendor(s) on the CSP(s) on a regular basis? This is to demonstrate compliance with information security requirements mandated by Hutchison Ports.   *If applicable, for (i) only, please indicate the relevant sections when included in the service agreement.* |
| **Answer:** *[Please fill in your response]* |
|  | **In terms of data interoperability and portability, explain if there are any formal procedures or controls to:**   1. Cater for any Hutchison Port's data access request(s) by agreed means of communication (e.g. email, phone to designated persons) in the agreement(s). 2. Provide secure and standardized network protocols for import and export of data. 3. Maintain data interoperability by using industry-recognized data, file and system formats among virtualization platforms or moving application data between platforms. 4. Maintain data quality and integrity by working with CSP(s) to correct any data quality errors. 5. Prevent or control risk of vendor lock-in   *If applicable, for (iii) and (iv), please indicate the relevant sections when included in the service agreement.* |
| **Answer:** *[Please fill in your response]* |
| **Remote Access Security** |  | **Explain what formal procedures or controls are in place to protect the use of mobile devices or Bring Your Own Devices (BYOD) by employees to store or/and access data Hutchison Ports, e.g.:**   1. Hold awareness and training for employees and contractors on the acceptable usage and security requirements of mobile devices 2. Maintain an inventory for all mobile/BYOD devices 3. Manage mobile device management solution, including remote wipes during loss of devices 4. Enforce encryption for entire devices or sensitive data on all mobile devices 5. Enforce password policies for all mobile devices 6. Deploy latest security patches on all mobile devices in a timely manner |
| **Answer:** *[Please fill in your response]* |