APPENDIX B

BOOKING HOLDINGS INFORMATION SECURITY REQUIREMENTS

**These Booking Holdings Inc Information Security Requirements describe the baseline technical and organizational security measures incorporated in the Information Security Management System (ISMS) that Supplier shall, as a minimum, have in place as part of their security operationalization, to ensure that the confidentiality, integrity and availability of any data created, collected, received or otherwise obtained to provide the Services to BHI, including any personal data (in Booking Holdings Inc. Security Requirements referred to as “Data”), is sufficiently protected.**

In particular, the Supplier shall take security measures that include appropriate technical and organizational safeguards to protect personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security, such as where appropriate, encryption, pseudonymization and anonymization. These technical and organizational security measures must enable Supplier to identify their critical assets and prevent, detect, respond to and recover from any adverse events targeting them. In this way, the BHI Personal Data created, collected, received or otherwise obtained to provide the Services to BHI, shall be systematically managed, the associated security risk shall be minimized and business continuity shall be achieved by proactively limiting the impact of a potential Data Security Breach. Specifically, Supplier must conform with the following security baselines as a minimum:

**A. IDENTIFY: *Supplier has an organizational understanding for managing cybersecurity and IT risks to systems, people, assets, data, and capabilities*.**

**Asset Management**

* A comprehensive catalogue of physical devices, software platforms, applications and external systems is in place.
* There is a comprehensive classification of resources based on criticality and business value
* Organizational communication and data flows are mapped.
* Cybersecurity roles and responsibilities for the workforce and third party stakeholders are established.

**Business Environment**

* The organization’s role in the supply chain, critical infrastructure and industry is defined.
* Dependencies and resilience requirements for the delivery of critical services are defined.

**Governance**

* Fundamental organizational cybersecurity policies, roles and responsibilities are defined.
* Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
* Policies regarding the compelled disclosure of personal data are defined.
* Governance and risk management processes address cybersecurity, IT, business risks and compliance.
* In case Supplier is under periodic external audits focused on IT risks, the resulting assurance reports (SOC1 (e.g. ISAE3402 Type 2), SOC2, or equivalent) shall be provided to BHI. In case Supplier is not periodically audited by an external independent party, BHI reserves the right to audit in case such a need arises.

**Risk Assessment**

* Asset vulnerabilities and internal and external threats are identified.
* Risk is determined based on the vulnerabilities and threats and their impact and likelihood.
* Risk response is defined and prioritized accordingly.

**Risk Management Strategy**

* Risk management processes are established and managed in line with a defined risk tolerance.

**Supply Chain Risk Management**

* Cyber supply chain risk management processes are established and applied to third party partners.
* Contracts with third party partners are utilized for meeting the organization’s cybersecurity program requirements.

**B. PROTECT: *Supplier has developed and implemented appropriate safeguards to ensure delivery of critical services***

**Identity Management & Access Control**

* There is a defined process around the issuance, management, revocation and review of identities, (standard and privileged) credentials and their interconnection.
* Measures are in place to ensure that persons authorized to use data processing systems only have access to what they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during and after processing.
* Physical and remote access to assets is logged, managed and protected.
* Measures are taken to ensure that physical access is secure and controlled, such as the presence of security staff, documentation on the issue of keys, an access control system and monitoring systems such as alarm systems and/or video surveillance.
* Security checks conducted for external services that have physical or remote access.
* Special access protection for any server rooms is present.
* Logical and physical access permissions and authorization are managed based on the least privilege principle and through applying segregation of duties as needed.
* Network integrity is protected.
* Appropriate measures are implemented to prevent data processing systems from being used without authorization, such as password procedures, automated blocking, authorization rules for terminals and users and, securing external interfaces.
* The authentication level of users, devices and other assets is determined by the risk of the associated transaction.

**Awareness and Training**

* All users receive BHI required security training upon engagement and annually.
* Senior executives, privileged users, physical and cybersecurity stakeholders and third party stakeholders understand their roles and responsibilities.

**Data Security**

* Data-at-rest and data-in-transit are safeguarded using one of the following approved encryption algorithms and protocols:

| ENCRYPTION AT REST | | | ENCRYPTION IN TRANSIT | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Algorithm | Effective Security Bits[[1]](#footnote-0) | Type | Auth | Stream cipher | Stream cipher variant | Message authentication |
| AES-128 or greater | 128 or greater | Symmetric | ECDHE-ECDSA | AES256 | GCM[[2]](#footnote-1) | SHA 384 |
| RSA-3072 or greater | 128 or greater | Asymmetric | ECDHE-ECDSA | ChaCha20 | Poly 1305 | SHA 256 |
| ECC Curve25519 | 128 | Asymmetric\* | ECDHE-ECDSA | AES128 | GCM | SHA 256 |
| \*) ECC Curve25519 is not by itself an encryption algorithm, but is used in conjunction with a symmetric encryption algorithm such as AES. | | | ECDHE-ECDSA | AES128 | CCM 8[[3]](#footnote-2) | SHA 256 |
| ECDHE-ECDSA | AES128 | CCM | SHA 256 |

* Used certificates and keys are registered and secrets are protected.
* Controls are in place to protect against data leakage and exfiltration and/or accidental data destruction.
* Procedures are in place to protect against the accidental loss or destruction of data, such as backup procedures, separate storage places, an emergency concept, firewalls and anti-virus protection, uninterruptible power supplies, object protection, anti-theft measures, redundant air conditioning/cooling systems and fire protection.
* Asset management occurs through controlled removal, transfer and disposition of assets.
* Integrity checking is used for software and information integrity.
* Availability is supported by adequate capacity.
* Measures are implemented to ensure the pseudonymization, tokenization and encryption of personal data where appropriate.
* Data labelling measures are implemented to ensure that data collected for different purposes can be processed separately, such as a clear logical separation, user profiles, authorization concept, separation of test and production data.

**Information Protection Processes and Procedures**

* Security principles are incorporated in the baseline of IT systems configuration.
* A System Development Life Cycle (SDLC) is implemented for managing systems.
* Configuration and change management processes are established.
* Backups of information are performed and maintained.
* Data is destroyed in accordance with an information management policy and as per the applicable laws and regulations.
* Processes are in place for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing. A data (security) breach management process is established and can be readily applied if needed.
* Response and recovery plans are in place for incident management, business continuity and disaster recovery.
* Personnel screening and user (de-)provisioning are incorporated in HR processes.
* A threat and vulnerability management procedure is in place.

**Maintenance**

* Maintenance of assets is performed with approved tools and is being logged.
* Approved remote maintenance of assets is performed in a way that prevents unauthorized access and is being logged.

**Protective Technology**

* Log records are maintained and reviewed.
* Removable media are protected through both physical and logical access control and their use is restricted to authorized personnel.
* Systems are configured to provide only essential capabilities as per the principle of least functionality.
* Communications and control records are protected.
* Mechanisms are in place to support resilience under normal and adverse conditions.

**C. DETECT: *Supplier has developed and implemented appropriate activities to identify the occurrence of a cybersecurity event*.**

**Anomalies and Events**

* A baseline of network operations and data flows is established.
* Incident alert thresholds are established.
* Detected events are analyzed for determining the target and the methods utilized.
* Event data are aggregated and correlated for their impact to be determined.

**Security Continuous Monitoring**

* The network, physical environment and personnel and external supplier activities are monitored to detect potential cybersecurity events.
* Measures are implemented to ensure that it is possible to check and ascertain whether BHI Personal Data have been accessed, altered or removed from data processing systems, such as authorization rules, access rules and logging.
* Safeguards are in place to detect malicious and/or unauthorized code.
* Monitoring is performed for unauthorized personnel, connections, devices and software.
* Vulnerability scans are performed at regular intervals.

**Detection Processes**

* Roles and responsibilities for detection activities are defined.
* Detection activities comply with basic regulatory requirements and are being tested.
* Event detection information is communicated.

**D. RESPOND: *Supplier has developed and implemented appropriate activities to take action regarding a detected cybersecurity incident*.**

**Response Planning**

* A response plan is defined and executed during or after an incident.

**Communications**

* Incident response roles and responsibilities are defined and personnel accountability is clear.
* Criteria for incident reporting are established and followed.
* Information sharing and coordination with stakeholders are consistent with a response plan.

**Analysis**

* Alerts from the detection systems are monitored and investigated as needed.
* Forensics are performed when needed.
* The impact of an incident is determined and understood.
* Incident categorization is consistent with the response plan.
* Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization.

**Mitigation**

* Identified incidents are contained and mitigated.
* Vulnerabilities are mitigated or their risk acceptance is documented.

**Improvements**

* Response strategies are updated based on lessons learned through response plans.

**E. RECOVER: *Supplier has developed and implemented appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident*.**

**Recovery Planning**

* A recovery plan is defined and is executed during or after a cybersecurity incident.

**Improvements**

* Recovery strategies are updated based on lessons learned through recovery plans.

**Communications**

* Recovery activities are communicated to internal and external stakeholders.
* Reputation impact is determined and repaired after an incident

1. NIST. “Recommendation for Key Management: Part 1 – General.” Section 5.6.1.1 and Table 2, 2020, pp. 53-55, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final [↑](#footnote-ref-0)
2. IETF. “AES Galois Counter Mode (GCM) Cipher Suites for TLS.” 2008, https://tools.ietf.org/html/rfc5288 [↑](#footnote-ref-1)
3. IETF. “AES-CCM Cipher Suites for Transport Layer Security (TLS) - Section 3.” 2012, https://tools.ietf.org/html/rfc6655#section-3 [↑](#footnote-ref-2)